

日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT



別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application:

2000年 3月 2日

出願番号
Application Number:

特願2000-057077

出願人
Applicant(s):

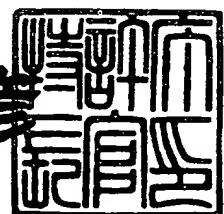
キヤノン株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

2000年 4月 14日

特許庁長官
Commissioner,
Patent Office

近藤 隆彦



出証番号 出証特2000-3027116

【書類名】 特許願
【整理番号】 4184060
【提出日】 平成12年 3月 2日
【あて先】 特許庁長官 近藤 隆彦 殿
【国際特許分類】 G06F 15/00
H04N 7/00
【発明の名称】 画像処理装置、方法及びシステム、並びに撮像装置、撮像方法、コンピュータ読み取り可能な記憶媒体
【請求項の数】 42
【発明者】
【住所又は居所】 東京都大田区下丸子3丁目30番2号キヤノン株式会社
内
【氏名】 若尾 聰
【発明者】
【住所又は居所】 東京都大田区下丸子3丁目30番2号キヤノン株式会社
内
【氏名】 岩村 恵市
【特許出願人】
【識別番号】 000001007
【住所又は居所】 東京都大田区下丸子3丁目30番2号
【氏名又は名称】 キヤノン株式会社
【代表者】 御手洗 富士夫
【電話番号】 03-3758-2111
【代理人】
【識別番号】 100090538
【住所又は居所】 東京都大田区下丸子3丁目30番2号キヤノン株式会社
内
【弁理士】
【氏名又は名称】 西山 恵三

【電話番号】 03-3758-2111

【選任した代理人】

【識別番号】 100096965

【住所又は居所】 東京都大田区下丸子3丁目30番2号キヤノン株式会
社内

【弁理士】

【氏名又は名称】 内尾 裕一

【電話番号】 03-3758-2111

【選任した代理人】

【識別番号】 100110009

【住所又は居所】 東京都大田区下丸子3丁目30番2号キヤノン株式会
社内

【弁理士】

【氏名又は名称】 青木 康

【電話番号】 03-3758-2111

【選任した代理人】

【識別番号】 100069877

【住所又は居所】 東京都大田区下丸子3丁目30番2号キヤノン株式会
社内

【弁理士】

【氏名又は名称】 丸島 儀一

【電話番号】 03-3758-2111

【先の出願に基づく優先権主張】

【出願番号】 平成11年特許願第 63174号

【出願日】 平成11年 3月10日

【手数料の表示】

【予納台帳番号】 011224

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9908388

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 画像処理装置、方法及びシステム、並びに撮像装置、撮像方法
、コンピュータ読み取り可能な記憶媒体

【特許請求の範囲】

【請求項1】 デジタル画像と秘密情報を用いて所定の演算を行う演算手段と、

前記演算手段の出力を用いて、前記デジタル画像に対する不正な処理を検出するための署名データを生成する生成手段とを具備することを特徴とする画像処理装置。

【請求項2】 請求項1において、前記演算手段は、前記デジタル画像と前記秘密情報を用いて逆演算可能な演算を行うことを特徴とする画像処理装置。

【請求項3】 請求項1若しくは2において、前記生成手段は、前記演算手段の演算結果に対して、逆演算の困難な演算を行うことを特徴とする画像処理装置。

【請求項4】 請求項3において、前記逆演算の困難な演算は、ハッシュ関数を用いた演算であることを特徴とする画像処理装置。

【請求項5】 請求項3において、前記一方向性関数は、共通鍵暗号を実現する演算であることを特徴とする画像処理装置。

【請求項6】 請求項1～5の何れかにおいて、前記生成手段は、前記デジタル画像毎に、該デジタル画像に対応する署名データを生成することを特徴とする画像処理装置。

【請求項7】 請求項1～6の何れかにおいて、前記生成手段は、前記演算手段の出力を用いて、前記デジタル画像に対する不正な処理を検出するため署名データを生成するプログラムに従って前記デジタル画像に対応する署名データを生成することを特徴とする画像処理装置。

【請求項8】 請求項1～7の何れかにおいて、前記秘密情報は、前記画像処理装置を識別するための情報であることを特徴とする画像処理装置。

【請求項9】 請求項1～7の何れかにおいて、前記秘密情報は、前記画像

処理装置と接続可能な外部装置を識別するための情報であることを特徴とする画像処理装置。

【請求項10】 請求項1～7の何れかにおいて、前記秘密情報は、前記画像処理装置と接続可能な外部装置を使用するユーザを識別するための情報であることを特徴とする画像処理装置。

【請求項11】 請求項1～10の何れかにおいて、前記署名データの生成に必要な演算の少なくとも一部を、前記画像処理装置に接続された外部装置に演算させることを特徴とする画像処理装置。

【請求項12】 請求項1～11の何れかにおいて、前記デジタル画像は、圧縮符号化されていることを特徴とする画像処理装置。

【請求項13】 請求項1～12の何れかにおいて、前記画像処理装置は更に、前記デジタル画像を生成する撮像部を具備することを特徴とする画像処理装置。

【請求項14】 請求項1～13の何れかにおいて、前記画像処理装置は更に、前記デジタル画像と前記署名データとを出力可能なデジタルインターフェースを具備することを特徴とする画像処理装置。

【請求項15】 請求項1～14の何れかにおいて、前記画像処理装置は更に、前記前記デジタル画像データと前記署名データとを所定の記録媒体に記録する記録手段を具備することを特徴とする画像処理装置。

【請求項16】 デジタル画像と秘密情報とを用いて所定の演算を行う演算手段と、

前記演算手段の出力と、前記デジタル画像に対する不正な処理を検出するための署名データとを比較して前記デジタル画像に対する不正な処理の有無を検出する検出手段とを具備することを特徴とする画像処理装置。

【請求項17】 請求項16において、前記演算手段は、前記デジタル画像と前記秘密情報とを用いて逆演算可能な第1の演算を行うことを特徴とする画像処理装置。

【請求項18】 請求項17において、前記演算手段は、前記第1の演算の結果に対して、一方向関数を用いた第2の演算を行うことを特徴とする画像処理

装置。

【請求項19】 請求項16～18の何れかにおいて、前記画像処理装置は、前記デジタル画像毎に、該デジタル画像に対する不正な処理の有無を検出することを特徴とする画像処理装置。

【請求項20】 請求項16～19の何れかにおいて、前記検出手段は、前記演算手段の出力と前記署名データとを比較して前記デジタル画像に対する不正な処理の有無を検出するプログラムに従って前記デジタル画像に対する不正な処理の有無を検出することを特徴とする画像処理装置。

【請求項21】 請求項16～20の何れかにおいて、前記画像処理装置は更に、前記検出手段の検出結果を表示する表示手段を具備することを特徴とする画像処理装置。

【請求項22】 デジタル画像と秘密情報とを用いて所定の演算を行う第1の演算手段と、

前記第1の演算手段の出力を用いて、該デジタル画像に対する不正な処理を検出するための署名データを生成する生成手段とを具備する第1の画像処理装置と、

前記デジタル画像と前記秘密情報とを用いて所定の演算を行う第2の演算手段と、

前記第2の演算手段の出力と前記署名データとを比較して該デジタル画像に対する不正な処理の有無を検出する検出手段とを具備する第2の画像処理装置により構成することを特徴とする画像処理システム。

【請求項23】 デジタル画像と秘密情報とを用いて所定の演算を行い、該演算結果を用いて、前記デジタル画像に対する不正な処理を検出するための署名データを生成することを特徴とする画像処理方法。

【請求項24】 デジタル画像と秘密情報とを用いて所定の演算を行い、該演算結果と、前記デジタル画像に対する不正な処理を検出するための署名データとを比較して前記デジタル画像に対する不正な処理の有無を検出することを特徴とする画像処理方法。

【請求項25】 デジタル画像と秘密情報とを用いて所定の演算を行う手

順と、

該演算結果を用いて、前記デジタル画像に対する不正な処理を検出するための署名データを生成する手順とを実行させるためのプログラムを記憶したことを特徴とするコンピュータ読み取り可能な記憶媒体。

【請求項26】 デジタル画像と秘密情報とを用いて所定の演算を行う手順と、

該演算結果と、前記デジタル画像に対する不正な処理を検出するための署名データとを比較して前記デジタル画像に対する不正な処理の有無を検出する手順とを実行させるためのプログラムを記憶したことを特徴とするコンピュータ読み取り可能な記憶媒体。

【請求項27】 デジタル画像を生成する撮像手段と、

前記デジタル画像と秘密情報とを用いて所定の演算を行い、該デジタル画像に対する不正な処理を検出するための署名データを生成する生成手段とを具備することを特徴とする撮像装置。

【請求項28】 請求項27において、前記生成手段は、前記デジタル画像と前記秘密情報とを用いて逆演算可能な第1の演算を行うことを特徴とする画像処理装置。

【請求項29】 請求項28において、前記生成手段は、前記第1の演算の結果に対して一方向関数を用いた第2の演算を行うことを特徴とする画像処理装置。

【請求項30】 請求項29において、前記一方向性関数は、ハッシュ関数であることを特徴とする撮像装置。

【請求項31】 請求項29において、前記一方向性関数は、共通鍵暗号を実現する関数であることを特徴とする撮像装置。

【請求項32】 請求項29において、前記生成手段は、前記撮像手段が前記デジタル画像を生成する毎に、該デジタル画像に対応する署名データを生成することを特徴とする撮像装置。

【請求項33】 請求項27～32の何れかにおいて、前記生成手段は、前記撮像手段により生成されたデジタル画像と秘密情報とを用いて所定の演算を

行い、該デジタル画像に対する不正な処理を検出するための署名データを生成するプログラムに従って前記デジタル画像に対応する署名データを生成することを特徴とする撮像装置。

【請求項34】 請求項27～33の何れかにおいて、前記秘密情報は、前記撮像装置を識別するための情報であることを特徴とする撮像装置。

【請求項35】 請求項27～33の何れかにおいて、前記秘密情報は、前記撮像装置と接続可能な外部装置を識別するための情報であることを特徴とする撮像装置。

【請求項36】 請求項27～33の何れかにおいて、前記秘密情報は、前記撮像装置と接続可能な外部装置を使用するユーザを識別するための情報であることを特徴とする撮像装置。

【請求項37】 請求項27～36の何れかにおいて、前記署名データの生成に必要な演算の少なくとも一部を、前記撮像装置に接続された外部装置に演算させることを特徴とする撮像装置。

【請求項38】 請求項27～37の何れかにおいて、前記デジタル画像は、圧縮符号化されていることを特徴とする撮像装置。

【請求項39】 請求項27～38の何れかにおいて、前記撮像装置は更に、前記デジタル画像と前記署名データとを出力可能なディジタルインターフェースを具備することを特徴とする撮像装置。

【請求項40】 請求項27～39の何れかにおいて、前記撮像装置は更に、前記前記デジタル画像と前記署名データとを所定の記録媒体に記録する記録手段を具備することを特徴とする撮像装置。

【請求項41】 デジタル画像を撮像し、
該デジタル画像と秘密情報を用いて所定の演算を行い、
該デジタル画像に対する不正な処理を検出するための署名データを生成することを特徴とする撮像方法。

【請求項42】 撮像部により撮像されたデジタル画像と、秘密情報を用いて所定の演算を行う手順と、

該デジタル画像に対する不正な処理を検出するための署名データを生成する

手順とを実行させるためのプログラムを記憶したことを特徴とするコンピュータ読み取り可能な記憶媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、画像処理装置、方法及びシステム、並びに撮像装置、撮像方法、コンピュータ読み取り可能な記憶媒体に関し、特に、デジタル画像情報の著作権を保護するための技術に関するものである。

【0002】

【従来の技術】

近年、撮影した画像を従来の銀塩写真や8mmフィルムに記録するのではなく、デジタルデータとして記録媒体に記録する画像入力装置（例えば、デジタルカメラ）が実用化されている。

【0003】

【発明が解決しようとする課題】

ところが、通常、デジタルデータは、アナログデータと異なり加工が容易で、修正、改竄、偽造、合成等を簡単に行うことができる。このため、デジタルデータは、銀塩写真等と比較して信憑性が低く、証拠能力に乏しいという問題があった。

【0004】

このような問題を解決するために、デジタルデータに対する修正、改竄、偽造、合成等を検出するための技術が提案されている。例えば、この技術の一例として、ハッシュ関数と公開鍵暗号方式とを組み合わせたシステムが提案されている。

【0005】

以下、図28を用いて従来のシステムを説明する。公開鍵暗号方式とは、暗号鍵と復号鍵とが異なり、暗号鍵を公開し、復号鍵を秘密に保持する方式である。

【0006】

まず、送信側（出力側）の構成と動作について説明する。

- ①デジタルデータMをハッシュ関数Hを用いて圧縮し、一定長の出力hを演算する。
- ②暗号鍵Keを用いて上述のhを暗号化し、出力sを求める。この出力sをデジタル署名データと呼ぶ。
- ③出力回路は、デジタル署名データsとデジタルデータMとを一組として出力する。

【0007】

次に、受信側（検出側）構成と動作について説明する。

- ④デジタルデータMとそれに対応するデジタル署名データsとを入力する。
- ⑤デジタル署名データsを暗号鍵Keに対応する復号鍵Kdで復号し、出力h'を生成する。
- ⑥デジタルデータMを送信側と同じハッシュ関数Hを用いて演算し、出力h'を求める。
- ⑦比較回路は、⑤で求めた出力h'を⑥で求めた出力h'を比較し、一致すれば入力されたデジタルデータMを不正な処理のされていない正当なデータであると判断し、不一致であれば不正な処理のされたデータと見なす。

【0008】

このように従来のシステムでは、ハッシュ関数Hと暗号鍵Keにより生成したデジタル署名データsを用いて、デジタルデータMに対する修正、改竄、偽造、合成等を検出していた。

【0009】

しかしながら、上述のシステムには次のような問題がある。

【0010】

まず、公開鍵暗号方式の暗号化回路及びその復号化回路は、回路構成が複雑であり、小型化が難しいという問題がある。また、それらの回路の演算量は膨大であり、処理時間が長くなるという問題もある。特に、公開鍵暗号方式は、べき乗演算と剰余演算とが必要であり、共通鍵暗号方式（暗号鍵と復号鍵とが同一となる暗号方式）に比べて演算が複雑且つ膨大となるため、処理速度の高速化が大変難しい。つまり、従来のシステムでは、処理速度の高速化とシステムの小型化の

双方を両立させることは難しいという問題がある。

【0011】

又、処理速度を早くするためには、より高性能のC P U（中央演算処理装置）とより大容量のメモリとを用いて、ハードウェアの性能を向上させる必要がある。しかしながら、このような構成では、システム全体の大規模化やコストアップを招くだけあり、安価で小型で高速なシステムをユーザに提供することはできない。

【0012】

以上の背景から本出願の発明の目的は、デジタルデータの著作権を保護を、簡単な構成で、安価に且つ安全に実現することのできる画像処理装置、方法及びシステム、並びに撮像装置、撮像方法、コンピュータ読み取り可能な記憶媒体を提供することである。

【0013】

【課題を解決するための手段】

上述のような目的を達成するために、本発明の画像処理装置は、デジタル画像と秘密情報とを用いて所定の演算を行う演算手段と、前記演算手段の出力を用いて、前記デジタル画像に対する不正な処理を検出するための署名データを生成する生成手段とを具備することを特徴とする。

【0014】

又、本発明の画像処理装置は、デジタル画像と秘密情報とを用いて所定の演算を行う演算手段と、前記演算手段の出力と、前記デジタル画像に対する不正な処理を検出するための署名データとを比較して前記デジタル画像に対する不正な処理の有無を検出する検出手段とを具備することを特徴とする。

【0015】

又、本発明の画像処理システムは、デジタル画像と秘密情報とを用いて所定の演算を行う第1の演算手段と、前記第1の演算手段の出力を用いて、該デジタル画像に対する不正な処理を検出するための署名データを生成する生成手段とを具備する第1の画像処理装置と、前記デジタル画像と前記秘密情報とを用いて所定の演算を行う第2の演算手段と、前記第2の演算手段の出力と前記署名デ

ータとを比較して該デジタル画像に対する不正な処理の有無を検出する検出手段とを具備する第2の画像処理装置とにより構成することを特徴とする。

【0016】

又、本発明の画像処理方法は、デジタル画像と秘密情報とを用いて所定の演算を行い、該演算結果を用いて、前記デジタル画像に対する不正な処理を検出するための署名データを生成することを特徴とする。

【0017】

又、本発明の画像処理方法は、デジタル画像と秘密情報とを用いて所定の演算を行い、該演算結果と、前記デジタル画像に対する不正な処理を検出するための署名データとを比較して前記デジタル画像に対する不正な処理の有無を検出することを特徴とする。

【0018】

又、本発明のコンピュータ読み取り可能な記憶媒体は、デジタル画像と秘密情報とを用いて所定の演算を行う手順と、該演算結果を用いて、前記デジタル画像に対する不正な処理を検出するための署名データを生成する手順とを実行させるためのプログラムを記憶したことを特徴とする。

【0019】

又、本発明のコンピュータ読み取り可能な記憶媒体は、デジタル画像と秘密情報とを用いて所定の演算を行う手順と、該演算結果と、前記デジタル画像に対する不正な処理を検出するための署名データとを比較して前記デジタル画像に対する不正な処理の有無を検出する手順とを実行させるためのプログラムを記憶したことを特徴とする。

【0020】

又、本発明の撮像装置は、デジタル画像を生成する撮像手段と、前記デジタル画像と秘密情報とを用いて所定の演算を行い、該デジタル画像に対する不正な処理を検出するための署名データを生成する生成手段とを具備することを特徴とする。

【0021】

又、本発明の撮像方法は、デジタル画像を撮像し、該デジタル画像と秘密

情報を用いて所定の演算を行い、該ディジタル画像に対する不正な処理を検出するための署名データを生成することを特徴とする。

【0022】

又、本発明のコンピュータ読み取り可能な記憶媒体は、撮像部により撮像されたディジタル画像と、秘密情報とを用いて所定の演算を行う手順と、該ディジタル画像に対する不正な処理を検出するための署名データを生成する手順とを実行させるためのプログラムを記憶したことを特徴とする。

【0023】

【発明の実施の形態】

以下、本発明の画像処理装置、方法及びシステム、並びに撮像装置、撮像方法、コンピュータ読み取り可能な記憶媒体について図面を用いて詳細に説明する。

【0024】

(基本構成)

まず、図1を用いて、各実施例に共通するディジタル画像検証システムの基本構成と処理手順とについて説明する。このシステムは、ディジタル画像データからディジタル署名データを生成するディジタル画像入力装置10と、そのディジタル署名データを用いてディジタル画像データに対する不正な処理を検出する画像検証装置20とからなる。各装置は、ネットワーク（例えば、インターネット、電話回線網、移動体通信網等）、各機器に共通のディジタルインターフェース、取り外し可能な記憶媒体（例えば、光ディスク、磁気ディスク、光磁気ディスク、半導体メモリ等）を介して接続される。

【0025】

尚、図1において、画像入力装置10と画像検証装置20とは、同一の秘密情報S12を共有する。この秘密情報S12は、読み出し専用の記録媒体等に記録され、外部に漏れることがないように管理する。

【0026】

まず、画像入力装置10は、ディジタル画像データP11と秘密情報S12とに基づいて、ディジタル署名データh13を生成する。具体的に説明すると、画像入力装置10は、秘密情報S12を用いてディジタル画像データP11に所定

の操作（例えば、付加、多重、或いは合成）を加えた後、その結果を一方向性関数（例えば、ハッシュ関数等の逆関数の生成が困難或いは不可能な関数）で演算し、その演算結果からディジタル署名データ h_{13} を生成する。このディジタル署名データ h_{13} は、対応するディジタル画像データ P_{11} と共に一時的に記録され、必要に応じて外部出力される。

【0027】

このような処理によって得られたディジタル署名データ h_{13} は、ディジタル画像データ P_{11} と秘密情報 S_{12} とに対して固有の情報となる。従って、秘密情報 S_{12} と所定の操作とを知らなければ、ディジタル画像データ P_{11} に対応するディジタル署名データ h_{13} を不正に作り出すことはできないため、ディジタル署名データ h_{13} に基づいてディジタル画像データ P_{11} の正当性を安全に検証することができる。又、一方向性関数の性質により、ディジタル署名データ h_{13} から元のデータ（即ち、秘密情報 S_{12} を用いて所定の操作を加えたディジタル画像データ P_{11} ）を知ることもできないため、ディジタル署名データ h_{13} に基づいてディジタル画像データ P_{11} の正当性（或いは、完全性（*integrity*）ともいう）を安全に検証することができる。

【0028】

次に、画像検証装置 20 は、ディジタル画像データ P'_{21} と共にディジタル署名データ h'_{23} を外部入力する。画像検証装置 20 は、ディジタル画像データ P'_{21} と秘密情報 S_{22} （上述の秘密情報 S_{12} と同一の情報である）とを用いて画像入力装置 10 と同様の処理を行い、ディジタル署名データ h''_{24} を生成する。

【0029】

このディジタル署名データ h''_{24} は、ディジタル画像データ P'_{21} と共に外部入力されたディジタル署名データ h'_{23} と比較される。両者が一致した場合、画像検証装置 20 は、ディジタル画像データ P'_{21} を正当なデータであると判断する。一方、ディジタル画像データ P'_{21} が外部入力される前に不正に処理されていた場合、両者は不一致となる。この場合、画像検証装置 20 は、ディジタル画像データ P'_{21} を不正に処理されたデータであると判断する。

【0030】

このような手順により、画像検証処装置20は、外部入力されたデジタル画像データP'21に対して不正な処理（例えば、修正、改竄、偽造、合成等の改変処理）が施されているか否かを検出することができる。

【0031】

以上のように、本実施例では、公開鍵暗号方式のような複雑な暗号化技術を用いることなく、簡単で安価な回路構成と少ない演算量で高速にデジタル署名データを生成することができる。そして、このデジタル署名データにより、デジタル画像データの著作権を保護し、該デジタル画像データに対する不正な処理（修正、改竄、偽造、合成等の改変処理）を確実に検出することができる。

【0032】

次に、図2に示す画像入力装置10及び画像検証装置20の基本的な構成について詳細に説明する。

【0033】

(1) 画像入力装置の構成

図2は、画像入力装置10の構成の一例を示す図である。ここで、画像入力装置10は、デジタルカメラ、カメラ一体型デジタルレコーダ、スキャナ等の撮像機能を有する電子機器である。

【0034】

図2において、撮像部201は、CCDやレンズ等からなり、被写体の光学像を電気信号に変換し、その電気信号を更に所定フォーマットのデジタル画像データに変換する。作業用メモリ202は、デジタル画像データ等を一時的に保管し、デジタル画像データに対する高能率符号化処理、後述のデジタル署名データの生成等に使用される。

【0035】

記録再生部203は、取り外し可能な記録媒体（例えば、光ディスク、磁気ディスク、光磁気ディスク、半導体メモリ等）に、撮像部201により生成され、高能率符号化されたデジタル画像データとそれに対応するデジタル署名データとを一組として記録する。駆動部204は、撮像部201や記録再生部203

の機械的動作を制御する。

【0036】

外部インターフェース部205は、ネットワーク（例えば、インターネット、電話回線網、移動体通信網等）に接続可能なディジタルインターフェースであり、デジタル署名データを付加したディジタル画像データを、所定の外部装置に送信する。

【0037】

制御／演算部206は、ROM207に格納されている各種のプログラムに従って画像入力装置10全体の動作を制御する制御回路210、ディジタル画像データを高能率符号化する（例えば、DCT変換やウェーブレット変換されたディジタル画像データを量子化し、可変長符号化する）画像処理回路211、後述のディジタル署名データの生成に必要なハッシュ関数演算や各種の演算処理を行う演算回路212、ディジタル署名データの生成に必要な秘密情報（例えば、画像入力装置10を識別するためのID情報等）を格納するメモリ213、演算回路212に必要な乱数を生成する乱数発生回路214を含む。

【0038】

ROM207は読み出し専用メモリであり、画像入力装置10全体の動作を制御するプログラム、画像処理を制御するプログラム、ディジタル署名データの生成処理を制御するプログラム等を格納している。操作部208は、ユーザからの各種の指示を受け付け、その指示に対応する制御信号を制御／演算部206に供給する。

【0039】

(2) 画像検証装置の構成

図3は、画像検証装置20の構成の一例を示す図である。ここで、画像検証装置20は、パーソナルコンピュータ、ワークステーション等の情報処理装置やそれらに接続可能な拡張ボードである。

【0040】

図3において、外部インターフェース部301は、ネットワークからディジタル署名データを付加したディジタル画像データ（ここで、ディジタル画像データは

、高能率符号化されている)を入力するデジタルインターフェースである。又、外部インターフェース部301は、取り外し可能な記録媒体とも接続可能である。そして、その記録媒体に記録されたデジタル画像データをデジタル署名データと共に入力する。

【0041】

作業用メモリ302は、デジタル画像データ等を一時的に保管し、デジタル画像データに対する伸長復号処理、後述のデジタル署名データの生成等に使用される。

【0042】

制御／演算部303は、ROM305に格納されている各種のプログラムに従って画像検証装置20全体の動作を制御する制御回路310、デジタル画像データを伸長復号する(例えば、可変長復号し、逆量子化した後、逆DCT変換や逆ウェーブレット変換する)画像処理回路311、後述のデジタル署名データの生成に必要なハッシュ関数演算やデジタル画像データを検証するための演算処理を行う演算回路312、デジタル署名データの生成に必要な秘密情報を格納するメモリ313、演算回路312に必要な乱数を生成する乱数発生回路314を含む。

【0043】

表示部304は、デジタル画像データを視覚的に表示する。又、表示部304は、そのデジタル画像データの検証結果をユーザに視覚的に表示する。尚、表示部304は、画像検証装置20と取り外し可能である。

【0044】

ROM305は、読み出し専用メモリであり、画像検証装置20全体の動作を制御するプログラム、画像処理を制御するプログラム、デジタル画像データの検証処理を制御するプログラムを格納している。操作部306は、ユーザからの各種の指示を受け付け、その指示に対応する制御信号を制御／演算部303に供給する。

【0045】

以下、第1～第6の実施例では、図2の画像入力装置10が、デジタル画像

データと秘密情報とに基づいて、デジタル署名データを生成する手順について詳細に説明する。

【0046】

又、第7～第12の実施例では、図4の画像検証装置20が、画像入力装置10にて生成されたデジタル署名データに基づいて、デジタル画像データの正当性を検証する手順について詳細に説明する。

【0047】

(第1の実施例)

第1の実施例では、画像入力装置10が、機器固有の秘密情報Sとハッシュ関数とを用いてデジタル署名データhを生成する処理について説明する。具体的に説明すると、デジタル画像データPと秘密情報Sとを用いて予め定められた規則の演算を行い、ハッシュ関数を用いてその演算結果を演算し、その演算結果をデジタル画像データPに対するデジタル署名データhとする。

【0048】

図4は、第1の実施例の処理手順を説明するフローチャートである。以下、図4を用いて、デジタル署名データhを生成する手順を説明する。

【0049】

ステップS401において、操作部208は、ある被写体の光学像を撮像するか否かを指示する。撮像が指示された場合、制御／演算部206はステップS402を実行する。

【0050】

ステップS402において、撮像部201は、被写体の光学像を電気信号に変換し、その電気信号を更に所定フォーマットのデジタル画像データPを生成する。その後、デジタル画像データPは、作業用メモリ202に格納される。

【0051】

ステップS403において、制御／演算部206（に含まれる画像処理回路211）は、作業用メモリ202に格納されたデジタル画像データPを1画面分の静止画像毎に高能率符号化する。1つの静止画像を高能率符号化する手法として例えば、DCT変換方式（具体的には、複数画素からなるブロック毎にDCT

変換、量子化及び可変量符号化する方式)、ウェーブレット変換方式(具体的には、複数画素からなるブロック毎にウェーブレット変換、量子化及び可変長符号化する方式)、JPEG方式、JBIG方式、MH方式、MMR方式、MPEG方式等を用いてもよい。尚、以下の実施例では、JPEG方式を用いて高能率符号化する場合について説明する。

【0052】

ステップS404において、制御／演算部206は、画像入力装置10の持つ秘密情報Sをメモリ213から読み出す。

【0053】

ステップS405において、制御／演算部206(に含まれる演算回路212)は、上述の秘密情報Sと例えばJPEG方式で高能率符号化されたディジタル画像データP(以下、JPEGデータと称する)とを用いて、予め定められた規則に基づく所定の演算を行う。

【0054】

ここで、秘密情報Sと所定の演算処理について説明する。

【0055】

まず、秘密情報Sとは、画像入力機器10の製造時に設定される機器固有の情報であり、一般に公開されることのない情報である。この秘密情報Sは、外部から容易に入手することができないように制御／演算部206の内部に組み込まれている。以下、第1の実施例では、上述の秘密情報Sを例えば“11111111”として説明する。

【0056】

次に、上述の所定の演算処理について図5を用いて説明する。所定の演算処理とは、あるJPEGデータ列から所定の位置のバイトデータを選択した後、そのバイトデータと秘密情報Sとをビット毎に排他的論理和演算し、そのバイトデータを別のデータに変換する処理のことである。ここで、所定の位置とは、JPEGデータ列上の任意の位置に設定することができるが、第1の実施例では最上位のバイトデータを演算対象として説明する。

【0057】

ステップS406において、制御／演算部206（に含まれる演算回路212）は、ハッシュ関数を用いて、所定の演算処理の施されたJPEGデータを演算し、デジタル署名データhを生成する。

【0058】

ここで、ハッシュ関数について説明する。

【0059】

ハッシュ関数Hとは、任意のビット長のデジタルデータMから、一定のビット長となる出力hを生成する機能を持つ。この出力hは、ハッシュ値と呼ばれる（又は、デジタル署名、メッセージダイジェスト、デジタル指紋等とも呼ばれる）。通常、ハッシュ関数には、一方向性と衝突耐性とが要求される。一方向性とは、ハッシュ値hが与えられた際に、 $h = H(M)$ となるデジタルデータMの算出が計算量的に困難であることを示す。又、衝突耐性とは、デジタルデータMが与えられた際に、 $H(M) = H(M')$ となるデジタルデータM' ($M \neq M'$) の算出および $H(M) = H(M')$ 且つ $M \neq M'$ となるデジタルデータM、M'の算出が計算量的に困難であることを示す。ハッシュ関数には、MD-2、MD-4、MD-5、SHA-1、RIPEMD-128、RIPEMD-160等の方式が知られている。第1の実施例では、MD-5方式を使用する例について説明する。尚、このMD-5方式を用いて生成されるデジタル署名データのビット長は128ビットとなる。

【0060】

ステップS407において、記録再生部203は、制御／演算部206にて生成されたデジタル署名データとそれに対応するデジタル画像データとを、取り外し可能な記録媒体に記録したり、ネットワークを介して他の機器に出力したりする。

【0061】

尚、図4に示す一連の処理手順を制御するプログラムは、ROM207に格納されている。このプログラムは、制御／演算部206（に含まれる制御回路210）によって読み出され、ユーザの撮像指示毎に起動される。これにより、デジタル画像Pを撮像する毎に、それに対応したデジタル署名データhを生成す

ることができる。

【0062】

以上説明したように第1の実施例では、高能率符号化されたディジタル画像データPと画像入力装置10に固有の秘密情報Sとを用いて所定の演算を行い、その演算結果をハッシュ関数で演算した結果が、ディジタル署名データhとなる。このように構成することによって、第1の実施例では、安全性も信頼性も高いディジタル署名データhを、従来のシステムに比べて非常に簡単な構成によって実現することができる。又、従来のシステムに比べて安価に構成することも、処理速度を高速化することもできる。

【0063】

この結果、秘密情報Sと所定の演算とを知らなければ、ディジタル画像データPに対応するディジタル署名データhを不正に作り出すことはできないため、ディジタル署名データhに基づいてディジタル画像データPの正当性を安全に検証することができる。又、一方向性関数の性質により、ディジタル署名データhから元のデータ（即ち、秘密情報Sを用いて所定の演算を行なったディジタル画像データP）を知ることもできないため、ディジタル署名データhからディジタル画像データPの正当性を安全に検証することができる。

【0064】

尚、第1の実施例では、秘密情報Sを画像入力装置10の製造時に設定された情報としたがそれに限るものではない。画像検証装置20の秘密情報と共有できるものであれば、乱数発生回路214が所定のアルゴリズムに基づいて生成したビット列でもよい。

【0065】

又、第1の実施例では、上述の所定の演算処理の一例として、JPGデータのバイトデータと秘密情報を排他的論理和演算する構成について説明したがそれには限るものではない。秘密情報Sを、高能率符号化されたディジタル画像データPの一部に付加、合成、あるいは多重する処理で且つ逆演算可能な処理であれば、いかなる演算処理であってもよい。

【0066】

又、第1の実施例では、デジタル画像データPとデジタル署名データhと同じタイミングで生成する手順について説明したがそれに限るものではない。デジタル画像データPを画像入力装置10から外部へ出力する前に必ずデジタル署名データhを生成する構成であれば、デジタル署名データhはどのタイミングで生成してもよい。例えば、デジタル画像データPを外部インターフェース205を介して外部に出力する場合には、一度記録媒体に格納した後、そのデジタル画像データPを外部へ出力する前に、デジタル署名データhを生成するようにしてもよい。但し、デジタル画像データPを取り外し可能な記録媒体に記憶する場合には、上述の手順でデジタル署名データhを生成する。

【0067】

(第2の実施例)

第2の実施例では、第1の実施例に比べてより安全性の高いデジタル署名データhを生成する手順について詳細に説明する。

【0068】

図6は、第2の実施例の処理手順を説明するフローチャートである。以下、図6を用いて、デジタル署名データhを生成する手順を説明する。

【0069】

ステップS601～S603の処理は、上述の第1の実施例のステップS401～S403と同様の処理としてその説明を省略する。

ステップS604において、制御／演算部206（に含まれる乱数発生回路214）は、所定の情報（例えば、高能率符号化されたデジタル画像データPのデータ量）を基にして、ビット長mの乱数Rを生成する。この乱数Rが第2の実施例の秘密情報Sである。

【0070】

次のステップS605～S606では、第2の実施例における所定の演算を説明する。

【0071】

ステップS605において、制御／演算部206（に含まれる演算回路212）は、図7に示すように、1画像分のJPEGデータを所定の大きさ（例えば1

28ビット長)のブロックD_i(i=1, 2, 3…n)に分割する。ここで、D₁を最上位ブロックとする。JPEGデータの総量が128の倍数にならない場合、128の倍数となるようにパディングする。例えば、図7に示すように、最後のブロックに“000…000”を付加する。

【0072】

ステップS606において、制御／演算部206(に含まれる演算回路212)は、上述の乱数Rと上述のn個のブロックとを用いて以下に示す手順の演算を行う。

【0073】

まず、制御／演算部206は、図8に示すように、乱数Rのビット数mをnビット(図7に示すブロックD_iの個数nと同じ)とする。例えば、m≥nの場合、最上位ビットからnビットまでのビット列を有効とし、それ以外のビット列を切り捨てる。又、m<nの場合、不足分のデータとして“111…111”を付加する。

【0074】

次に、制御／演算部206は、図9に示すように、各ブロックD₁～D_nと各乱数R₁～R_nとを用いて所定の演算を行う。具体的に説明すると、乱数RのビットR_iとブロックD_iの最下位ビットとの間で排他的論理和演算を行い、その演算をi=1～nまで繰り返す。

【0075】

ここで、ステップS606の演算は、乱数R_iとブロックD_iの最下位ビットとの間の排他的論理和演算としたがそれに限るものではない。各ブロックD_iの一部に秘密情報(ビット長mの乱数Rの一部)を付加、合成、多重する処理で且つ逆演算可能な処理であればいかなる演算処理であってもよい。

【0076】

ステップS607において、制御／演算部206(に含まれる演算回路212)は、ステップS606の出力をハッシュ関数で演算し、デジタル署名データhを生成する。尚、第2の実施例では、第1の実施例と同様に、MD-5方式のハッシュ関数を用いる。従って、デジタル署名データhのビット長は、128

ビットとなる。

【0077】

ステップS607の演算処理の一例について詳細に説明する。

【0078】

まず、制御／演算部206は、ステップS606の出力から1つまたは複数個のブロックDを選択する。その後、制御／演算部206は、選択されたブロックをハッシュ関数で演算し、デジタル署名データhを生成する。

【0079】

また、ステップS605～S607の演算処理の他の例について、図10～12を用いて詳細に説明する。

【0080】

制御／演算部206は、後述する3つの動作モードの何れか1つ又はこれらの組み合わることによりハッシュ値を求める。特に、第1のモードや第3のモードでは、あるブロック（1ブロックは、kビット）の演算結果を用いて他のブロックのハッシュ値を求めるため、より安全性の高いデジタル署名データhを生成することができる。又、前のブロックの演算結果が、次のブロックの演算結果に反映されるため、ブロック毎にJPEGデータの正当性を検証することもできる

【0081】

①第1のモード

第1のモードについて図10を用いて説明する。図10は、制御／演算部206の構成の一部を示す図である。

【0082】

図10において、演算回路212は、所定のビット単位でハッシュ関数演算を行うハッシュ関数回路1001と、ハッシュ関数回路1001の出力hの一部（Kビット）を記憶するレジスタ1002と、JPEGデータをKビットのブロックに分割する演算回路1003と、演算回路1003の出力とレジスタ1002の出力とを排他的論理和演算する演算回路1004とから構成される。

【0083】

ハッシュ関数回路1001の出力である128ビットのハッシュ値hの一部（Kビット）は、レジスタ1002に入力される。レジスタ1002には、例えば、ハッシュ値hの上位64ビットが一時的に格納される。

【0084】

レジスタ1002に格納されたKビットは、1ブロックのJPEGデータと排他的論理和演算され、その演算結果はハッシュ関数回路1001に供給される。

【0085】

上述の演算は、所定のブロックに達するまで、各ブロックに対して繰り返される。そして、その所定のブロックから求めたハッシュ値がデジタル署名データとして出力される。

【0086】

ここで、最初の演算では、レジスタ1002に初期値を格納しておく必要がある。その初期値は、例えば図13に示すように、乱数Rの下位Kビットを用いることができる。

【0087】

尚、ブロックD_iの大きさが64の倍数とならない場合には、例えば後述の第3のモードと組合せて余りのビット列を演算するように構成してもよい。

【0088】

②第2のモード

第2のモードについて図11を用いて説明する。図11は、制御／演算部206の構成の一部を示す図である。

【0089】

図11において、演算回路212は、所定のビット単位でハッシュ関数演算を行うハッシュ関数回路1101と、ハッシュ関数回路1101に必要な入力値を供給するレジスタ1102と、ハッシュ関数回路1101の出力hの一部（Kビット）を出力するセレクタ1103と、JPEGデータをKビットのブロックに分割する演算回路1104と、演算回路1104の出力とセレクタ1103の出力とを排他的論理和演算する演算回路1105とから構成される。

【0090】

ハッシュ関数回路1101は、乱数発生回路214にて生成された秘密情報（即ち、乱数R）を初期値とするレジスタ1102の値をハッシュ関数で演算する。

【0091】

ハッシュ関数回路1101の出力である128ビットのハッシュ値hは、セレクタ1103に入力される。セレクタ1103は、128ビットのハッシュ値hの内、例えば下位Kビットを出力する。このKビットは、次にハッシュ関数演算されるデータとしてレジスタ1102に格納される。

【0092】

上述の演算は、所定のブロックに達するまで、各ブロックに対して繰り返される。そして、その所定のブロックから求めたハッシュ値がディジタル署名データとして出力される。

【0093】

尚、最初のハッシュ関数演算に必要な初期値は、例えば図13に示すように、上述の乱数Rの下位Kビットを用いることができる。

【0094】

③第3のモード

第3のモードについて図12を用いて説明する。図12は、制御／演算部206の構成の一部を示す図である。

【0095】

図12において、演算回路212は、所定のビット単位でハッシュ関数演算を行うハッシュ関数回路1201と、ハッシュ関数回路1201に必要な入力値を供給するレジスタ1202と、ハッシュ関数回路1201の出力hの一部（Kビット）を出力するセレクタ1203と、PEGデータをKビットのブロックに分割する演算回路1204と、演算回路1204の出力とセレクタ1203の出力とを排他的論理和演算する演算回路1205とから構成される。

【0096】

ハッシュ関数回路1201は、乱数発生回路214にて生成された秘密情報を初期値とするレジスタ1202の値を順次ハッシュ関数演算する。

【0097】

ハッシュ関数回路1201の出力である128ビットのハッシュ値hは、セレクタ1203に入力される。セレクタ1203は、128ビットのハッシュ値hの内、例えば下位Kビットを出力する。このKビットは、1ブロックのJPEGデータと排他的論理和演算され、その演算結果の一部は再びレジスタ1202に格納される。

【0098】

上述の演算は、所定のブロックに達するまで、各ブロックに対して繰り返される。そして、その所定のブロックから求めたハッシュ値がディジタル署名データとして出力される。

【0099】

尚、最初のハッシュ関数演算に必要な初期値は、例えば図13に示すように、上述の乱数Rの下位Kビットを用いることができる。

【0100】

ステップS608において、記録再生部203は、制御／演算部206にて生成されたディジタル署名データhとそれに対応するディジタル画像データPとを取り外し可能な記録媒体に記録したり、ネットワークを介して他の機器に出力したりする。

【0101】

尚、図6に示す一連の処理手順を制御するプログラムは、ROM207に格納されている。このプログラムは、制御／演算部206（に含まれる制御回路210）によって読み出され、ユーザの撮像指示毎に起動される。

【0102】

以上のように第2の実施例では、ある長さの乱数Rから生成された秘密情報Sと高能率符号化されたディジタル画像データPとを用いて所定の演算を行い、その演算結果をハッシュ関数で演算してディジタル署名データhを生成する。このように構成することによって、第2の実施例では、従来のシステムに比べて安全性も信頼性も高いディジタル署名データhを簡単な構成によって実現することができる。又、従来のシステムに比べて安価に構成することも、処理速度を高速化

することもできる。

【0103】

又、第2の実施例では、ハッシュ関数演算を上述の動作モードの1つまたは複数を組み合わせて実現することにより、第1の実施例に比べてより安全性の高いディジタル署名データ生成アルゴリズムを提供することができる。

【0104】

更に、第2の実施例では、第1の実施例と同様に、ディジタル署名データhを用いて、ディジタル画像データPがどの画像入力装置にて撮像されたかを特定することもできる。

【0105】

(第3の実施例)

第1、第2の実施例では、ハッシュ関数を用いてディジタル署名データhを生成する手順について説明した。

【0106】

これに対して、第3の実施例では、ハッシュ関数ではなく、共通鍵暗号を用いてディジタル署名データhを生成する手順について詳細に説明する。

【0107】

図14は、第3の実施例の処理手順を説明するフローチャートである。以下、図14を用いて、ディジタル署名データhを生成する手順を説明する。

【0108】

ステップS1401～S1403の処理は、上述の第1の実施例のステップS401～S403と同様の処理としてその説明を省略する。

【0109】

ステップS1404において、制御／演算部206は、画像入力装置10の持つ固有の秘密情報Sをメモリ213から読み出す。第3の実施例では、“1111…1111”（128ビット）を秘密情報Sとして説明する。

【0110】

ステップS1405において、制御／演算部206（に含まれる演算回路212）は、作業用メモリ202に保持されたJPEGデータを共通鍵暗号方式に基

づいて暗号化する。ここで、JPEGデータを共通鍵暗号化する暗号鍵は、秘密情報Sから生成する。

【0111】

共通鍵暗号方式には現在様々なものが提案されているが、第3の実施例ではDES方式を用いる。DES方式を使用する場合、暗号鍵のビット長は56ビットであるので、秘密情報Sの上位56ビットを暗号鍵とする（図15参照）。ここで、この暗号鍵のビット長は、使用する共通鍵暗号方式の種類によって異なるものである。従って、FEAL-nX, MITSY, IDEAを使用する場合、暗号鍵は128ビットであるので、秘密情報Sの上位128ビットを暗号鍵とする。又、FEAL-n, MULTI 2を使用する場合、暗号鍵は64ビットであるので、秘密情報Sの上位64ビットを暗号鍵とする。

【0112】

ステップS1405における共通鍵暗号化処理について詳細に説明する。

【0113】

制御／演算部206は、後述する3つの動作モード（即ち、CBCモード、CFBモード、OFBモード）の何れか1つ又はこれらの組み合わせにより、JPEGデータを暗号化する。何れの動作モードにおいても、入力データを搅乱しながら暗号化することができるため、より安全性の高い暗号化処理を実現できる。

【0114】

① CBC (Cipher Block Chaining) モード

CBCモードを図16を用いて説明する。図16は、制御／演算部206の一部（即ち、演算回路212）を示す図である。

【0115】

図16において、演算回路212は、64ビット単位で暗号化を行う暗号化回路1601と、暗号化回路1601の出力を一時的に保持するレジスタ1602と、JPEGデータとレジスタ1602の出力とを排他的論理和演算する演算回路1603とから構成される。

【0116】

暗号化回路1601は、64ビットからなるブロック毎に、JPEGデータを

暗号化する。暗号化回路1601の出力は、レジスタ1602に一時的に格納される。レジスタ1602に格納された64ビットのデータは、次のブロックと排他的論理和演算され、その演算結果は暗号化回路1601に供給される。最終的に、全てのブロックを暗号化した結果が暗号データとして出力される。この暗号データの一部が、ディジタル署名データとなる。

【0117】

ここで、最初のブロックの暗号化では、レジスタ1602に初期値を格納しておく必要がある。その初期値は、例えば、秘密情報Sの下位64ビットを用いる（図15参照）。

【0118】

尚、ブロックの大きさが64の倍数とならない場合には、例えば後述のOFBモードと組合せて余りのビット列を暗号化するように構成してもよい。

【0119】

②OFB (Output Feedback) モード

OFBモードについて図17を用いて説明する。図17は、制御／演算部206の一部（即ち、演算回路212）を示す図である。

【0120】

図17において、演算回路212は、64ビット単位で暗号化を行う暗号化回路1701と、暗号化回路1701に必要な入力値を供給するレジスタ1702と、暗号化回路1701の出力を選択的に出力するセレクタ1703と、JPEGデータとセレクタ1703の出力とを排他的論理和演算する演算回路1704とから構成される。

【0121】

暗号化回路1701は、レジスタ1702に格納された64ビットのデータを暗号化する。暗号化回路1701の出力は、セレクタ1703に入力される。セレクタ1703は、例えば下位Kビットを出力する。このKビットは、次に暗号化されるデータとしてレジスタ1702に格納される。セレクタ1703から出力されたKビットは、JPEGデータの各ブロック（1ブロックは、Kビット）と排他的論理和演算され、その結果が暗号データとなる。この暗号データの一部

が、デジタル署名データ h となる。

【0122】

尚、最初の暗号化に必要な初期値は、例えば、秘密情報 S の下位 64 ビットを用いる（図 15 参照）。

【0123】

③ CFB (Cipher Feedback) モード

CFB モードについて図 18 を用いて説明する。図 18 は、制御／演算部 206 の一部（即ち、演算回路 212）を示す図である。

【0124】

図 18において、演算回路 212 は、64 ビット単位で暗号化を行う暗号化回路 1801 と、暗号化回路 1801 に必要な入力値を供給するレジスタ 1802 と、暗号化回路 1801 の出力を選択的に出力するセレクタ 1803 と、JPEG データとセレクタ 1803 の出力とを排他的論理和演算する演算回路 1804 とから構成される。

【0125】

暗号化回路 1801 は、レジスタ 1802 に格納された 64 ビットのデータを暗号化する。暗号化回路 1801 の出力は、セレクタ 1803 に入力される。セレクタ 1803 は、例えば下位 K ビットを出力する。セレクタ 1803 から出力された K ビットは、1 ブロック (K ビット) の JPEG データと排他的論理和演算され、その結果は再びレジスタ 1802 に格納される。最終的に、全てのブロックを処理した結果が暗号データとして出力される。この暗号データの一部が、デジタル署名データ h となる。

【0126】

尚、最初の暗号化に必要な初期値は、例えば、秘密情報 S の下位 64 ビットを用いる（図 15 参照）。

【0127】

ステップ S1406において、制御／演算部 206（に含まれる演算回路 212）は、ステップ S1405 にて生成された暗号データから特定のビット列をデジタル署名データとして抽出する。例えば、上述の暗号データの下位 128 ビ

ットをデジタル署名データとする。

【0128】

ステップS1407において、記録再生部203は、制御／演算部206（に含まれる演算回路212）にて生成されたデジタル署名データhとそれに対応するデジタル画像データPとを、取り外し可能な記録媒体に記録したり、ネットワークを介して他の機器に出力したりする。

【0129】

尚、図14に示す一連の処理手順を制御するプログラムは、ROM207に格納されている。このプログラムは、制御／演算部206（に含まれる制御回路210）によって読み出され、ユーザの撮像指示毎に起動される。

【0130】

以上のように第3の実施例では、秘密情報Sの一部から生成した暗号鍵と高能率符号化されたデジタル画像データPとを用いて共通鍵暗号方式による暗号化を行い、暗号化されたデータからデジタル署名データhを生成する。このように構成することにより、第3の実施例では、第1、第2の実施例に比べて安全性も信頼性も向上させたデジタル署名データを生成することができる。又、従来のシステムに比べて安価に構成することも、処理速度を高速化することもできる。

【0131】

又、第3の実施例では、デジタル署名データhを用いて、デジタル画像データがどの画像入力装置にて撮像されたかを特定することもできる。

【0132】

尚、第3の実施例では、秘密情報Sを“1111…1111”（128ビット）としたがこれに限るものではない。例えば、乱数発生回路214が所定のアルゴリズムに基づいて発生させた乱数とすることも可能である。但し、この秘密情報Sは画像検証装置20と共有される。

【0133】

（第4の実施例）

第3の実施例では、ハッシュ関数ではなく共通鍵暗号を用いてデジタル署名

データ h を生成する手順について説明した。

【0134】

これに対して、第4の実施例では、所定の演算（例えば、ビット挿入を含む逆演算可能な演算）を行い、その演算結果を共通鍵暗号方式で暗号化した後、暗号化されたデータからデジタル署名データ h を生成する手順について説明する。

【0135】

図19は、第4の実施例の処理手順を説明するフローチャートである。以下、図19を用いて、デジタル署名データ h を生成する手順を説明する。

【0136】

ステップ S1901～S1903 の処理は、上述の第1の実施例のステップ S401～S403 と同様の処理としてその説明を省略する。

【0137】

ステップ S1904～S1906 の処理は、上述の第2の実施例のステップ S604～S606 と同様の処理（即ち、秘密情報である乱数 R のビット R_i と JPEG データのブロック D_i を用いた排他的論理和演算）としてその説明を省略する。

【0138】

ここで、ステップ S1906 の演算は、上述のステップ S606 と同様に、乱数 R_i とブロック D_i の最下位ビットとの間の排他的論理和演算としたがそれに限るものではない。各ブロック D_i の少なくとも一部に秘密情報 S（ビット長 m の乱数 R）の一部を付加、合成、多重する処理で且つ逆演算可能な処理であれば、いかなる演算処理であってもよい。

【0139】

ステップ S1907において、制御／演算部 206（に含まれる演算回路 212）は、ステップ S1906 の出力を共通鍵暗号方式に従って暗号化する。ここで、制御／演算部 206 は、第3の実施例と同様に、DES 方式を利用するものとし、その暗号化に必要な暗号鍵は、ステップ S1904 で生成した秘密情報 S の上位 56 ビットとする（図20参照）。

【0140】

ステップS1907における暗号化処理について詳細に説明する。

【0141】

制御／演算部206は、上述した3つの動作モード（即ち、CBCモード、CFBモード、OFBモード）の何れか1つ又はこれらの組み合せ、乱数Rのビット R_i とJPEGデータのブロック D_i とを排他的論理和演算した結果を、順次暗号化する。何れの動作モードにおいても、入力データを搅乱しながら暗号化することができるため、より安全性の高い暗号化を実現できる。

【0142】

ステップS1908において、制御／演算部206（に含まれる演算回路212）は、ステップS1907にて生成された暗号データから特定のビット列をデジタル署名データ h として抽出する。例えば、暗号データの下位128ビットをデジタル署名データ h とする。

【0143】

ステップS1909において、記録再生部203は、制御／演算部206（に含まれる演算回路212）にて生成されたデジタル署名データ h とそれに対応するデジタル画像データ P とを、取り外し可能な記録媒体に記録したり、ネットワークを介して他の機器に出力したりする。

【0144】

尚、図19に示す一連の処理手順を制御するプログラムは、ROM207に格納されている。このプログラムは、制御／演算部206（に含まれる制御回路210）によって読み出され、ユーザの撮像指示毎に起動される。

【0145】

以上のように第4の実施例では、乱数Rから生成された秘密情報Sと高能率符号化されたデジタル画像データPとを用いて所定の演算を行い、その演算結果を共通鍵暗号方式により暗号化し、暗号化されたデータからデジタル署名データ h を生成する。このように構成することにより、第4の実施例では、第3の実施例に比べて安全性も信頼性も向上させたデジタル署名データを生成することができる。又、従来のシステムに比べて安価に構成することも、処理速度を高速化することもできる。

【0146】

又、第4の実施例では、デジタル署名データhを用いて、あるデジタル画像データPがどの画像入力装置にて撮像されたかを特定することもできる。

【0147】

(第5の実施例)

第1～第4の実施例では、画像入力装置10に固有の秘密情報Sに基づいて、デジタル署名データhを生成する構成について説明した。このような構成により第1～第4の実施例では、デジタル署名データhを用いて、あるデジタル画像データPがどの画像入力装置にて撮像されたものであるかを特定することができる。

【0148】

これに対して、第5の実施例では、外部装置（例えば、ICカード等）を画像入力装置10に接続し、この外部装置に固有の秘密情報Sに基づいて、デジタル署名データhを生成する構成について説明する。外部機器の持つ秘密情報Sは、例えば、画像入力装置10を識別するためのID情報、画像入力装置10を使用するユーザを識別するためのID情報とすることができます。このように構成することにより、第5の実施例では、デジタル署名データhを用いて、デジタル画像データがどの外部機器と接続された画像入力装置によって撮像されたものか、或いはどのユーザによって撮像されたものであるかを特定することができる。

【0149】

図21は、第5の実施例の処理手順を説明するフローチャートである。以下、図21を用いて、デジタル署名データhを生成する手順を説明する。

【0150】

ステップS2101において、画像入力装置10の制御/演算処理部206は、外部I/F部205に外部装置40が接続されているか否かを検出する。

【0151】

ステップS2102において、画像入力装置10と外部装置40とは、相互認証を行い、互いに正当なものであるかどうかをチェックする。

【0152】

図22を用いて、画像入力装置10と外部装置40との相互認証処理について説明する。

【0153】

画像入力装置10は、乱数発生回路214を用いて認証用の乱数aを発生させ、その乱数aを外部I/F部205を介して外部装置40に送信する。

【0154】

次に外部装置40の暗号化回路43は、認証用の暗号鍵を用いて乱数aをAに変換し、その暗号データAを外部I/F部41を介して画像入力装置10へ送信する。

【0155】

又、画像入力装置10の暗号化回路2201は、乱数aを認証用の暗号鍵を用いてA'に変換する。比較回路2202は、その暗号データA'を外部装置40から送信された暗号データAと比較し、それらが一致すれば外部装置40を認証する。

【0156】

同様にして、外部装置40は、乱数発生回路42を用いて認証用の乱数bを発生させ、その乱数bを外部I/F部205を介して画像入力装置10に送信する。

【0157】

次に画像入力装置10の暗号化回路2201は、認証用の暗号鍵を用いて乱数bをBに変換し、その暗号データBを外部I/F部205を介して外部装置40へ送信する。

【0158】

又、外部装置40の暗号化回路43は、乱数bを認証用の暗号鍵を用いてB'に変換する。比較回路44は、その暗号データB'を画像入力装置10から送信された暗号データBと比較し、それらが一致すれば画像入力装置10を認証する。

【0159】

双方が正常に認証された場合、外部装置40は、メモリ45に格納された秘密情報Sを外部I/F部41を介して画像入力装置10に送信する。

【0160】

ステップS2103～S2105の処理は、上述の第1の実施例のステップS401～S403と同様の処理としてその説明を省略する。

【0161】

ステップS2106において、制御／演算部206は、外部I/F部205を介して入力された秘密情報Sをメモリ213に格納する。

【0162】

ステップS2107において、制御／演算部206（に含まれる演算回路212）は、秘密情報SとJPEG方式で高能率符号化されたデジタル画像データP（以下、JPEGデータと称する）とを用いて、予め定められた規則に基づく所定の演算を行う。ここで、演算回路212は、第1の実施例のステップS405と同様の演算を行う。

【0163】

ステップS2108において、制御／演算部206（に含まれる演算回路212）は、ステップS2107の演算結果をハッシュ関数で演算し、その結果からデジタル署名データhを生成する。ここで、演算回路212は、第1の実施例のステップS406と同様の演算処理を行う。

【0164】

ステップS2109において、記録再生部203は、制御／演算部206にて生成されたデジタル署名データhとそれに対応するデジタル画像データPとを、取り外し可能な記録媒体に記録したり、ネットワークを介して他の機器に出力したりする。

【0165】

尚、図21に示す一連の処理手順を制御するプログラムは、ROM207に格納されている。このプログラムは、制御／演算部206（に含まれる制御回路210）によって読み出され、ユーザの撮像指示毎に起動される。これにより、デジタル画像を撮像する毎にその画像に対応したデジタル署名データhを生成

することができる。

【0166】

以上のように第5の実施例では、高能率符号化されたデジタル画像データPと外部装置40の有する秘密情報Sとを用いて所定の演算を行い、その演算結果をハッシュ関数で演算した後、その演算結果からデジタル署名データhを生成する。このように構成することにより、第5の実施例では、従来のシステムに比べて安全性も信頼性も向上させたデジタル署名データを生成することができる。又、従来のシステムに比べて安価に構成することも、処理速度を高速化することもできる。

【0167】

この結果、外部機器の秘密情報Sと所定の演算とを知らなければ、デジタル画像データPに対応するデジタル署名データhを不正に作り出すことはできないため、デジタル署名データhに基づいてデジタル画像データPの正当性を安全に検証することができる。又、一方向性関数の性質により、デジタル署名データhから元のデータ（即ち、秘密情報Sを用いて所定の演算を行なったデジタル画像データP）を知ることもできないため、デジタル署名データhからデジタル画像データPの正当性を安全に検証することができる。

【0168】

又、デジタル署名データhを用いて、デジタル画像データがどのユーザによって撮像されたかを特定することもできる。

【0169】

尚、第5の実施例では、デジタル署名データhを生成する手順を第1の実施例と同様の手順としたがそれに限るものではない。上述の第2～第4の実施例の何れも適用することができる。

【0170】

（第6の実施例）

第5の実施例では、画像入力装置10に外部装置40を接続し、この外部装置40の持つ固有の秘密情報に基づいてデジタル署名データを生成する構成について説明した。

【0171】

これに対して、第6の実施例では、画像入力装置10を外部装置40に接続し、この外部装置40に固有の秘密情報S2と画像入力装置10に固有の秘密情報S1の双方に基づいて、デジタル署名データhを生成する構成について説明する。このように構成することにより第6の実施例では、デジタル署名データhを用いて、デジタル画像データPがどの外部機器と接続されたどの画像入力装置によって撮像されたものか、或いはどのユーザが使用するどの画像入力装置によって撮像されたものであるかを特定することができる。

【0172】

図21を用いて第6の実施例の処理手順を詳細に説明する。

【0173】

ステップS2101において、画像入力装置10の制御/演算処理部206は、外部I/F部205に外部装置40が接続されているか否かを検出する。

【0174】

ステップS2102において、画像入力装置10と外部装置40とは、相互認証を行い、互いに正当なものであるかどうかをチェックする。

【0175】

ステップS2103～S2105の処理は、上述の第1の実施例のステップS401～S403と同様の処理としてその説明を省略する。

【0176】

ステップS2106において、制御/演算部206は、画像入力装置10の持つ秘密情報S1をメモリ213から読み出すと共に、外部装置40の持つ秘密情報S2を外部I/F部205を介して入力する。そして、これらの秘密情報S1、S2を結合させ、新しい秘密情報Sを生成する。

【0177】

ここで、画像入力装置10の秘密情報S1を例えば“1111”とし、外部装置40の秘密情報S2を例えば“0000”とすると、新たに生成される秘密情報Sは、例えば“11110000”となる。尚、第6の実施例では、2つの秘密情報を単に結合することにより新たな秘密情報Sを生成する場合について説明

したが、秘密情報 S から秘密情報 S₁，S₂を抽出できる演算であれば、いかなる演算であってもよい。

【0178】

ステップ S₂₁₀₇において、制御／演算部 206（に含まれる演算回路 212）は、秘密情報 S と JPEG 方式で高能率符号化されたデジタル画像データ P（以下、JPEG データと称する）とを用いて、予め定められた規則に基づく所定の演算を行う。ここで、演算回路 212 は、第 1 の実施例のステップ S₄₀₅と同様の演算を行う。

【0179】

ステップ S₂₁₀₈において、制御／演算部 206（に含まれる演算回路 212）は、ステップ S₂₁₀₇の演算結果をハッシュ関数で演算し、その結果からデジタル署名データ h を生成する。

【0180】

ステップ S₂₁₀₉において、記録再生部 203 は、制御／演算部 206 にて生成されたデジタル署名データ h とそれに対応するデジタル画像データ P とを、取り外し可能な記録媒体に記録したり、ネットワークを介して他の機器に出力したりする。

【0181】

尚、図 21 に示す一連の処理手順を制御するプログラムは、ROM 207 に格納されている。このプログラムは、制御／演算部 206（に含まれる制御回路 210）によって読み出され、ユーザの撮像指示毎に起動される。これにより、デジタル画像を撮像する毎にその画像に対応したデジタル署名データを生成することができる。

【0182】

以上説明したように、第 6 の実施例では、高能率符号化されたデジタル画像データ P と、画像入力装置 10 の秘密情報 S₁ と外部装置 40 の秘密情報 S₂ とから生成された秘密情報 S とを用いて所定の演算を行い、その演算結果をハッシュ関数で演算した後、その演算結果を用いてデジタル署名データ h を生成する。このように構成することにより、第 6 の実施例では、従来のシステムに比べて

安全性も信頼性も向上させたデジタル署名データを生成することができる。又、従来のシステムに比べて安価に構成することも、処理速度を高速化することもできる。

【0183】

又、デジタル署名データhを用いて、デジタル画像データがどの外部機器と接続された画像入力装置によって撮像されたものか、或いはどのユーザによって使用された画像入力装置にて撮像されたものかを特定することができる。

【0184】

尚、第6の実施例では、デジタル署名データhを生成する手順を第1の実施例と同様の手順としたがそれに限るものではない。上述の第2～第4の実施例の何れも適用することができる。

【0185】

(第7の実施例)

第7の実施例では、第1の実施例の画像入力装置10が生成したデジタル署名データhを用いて、デジタル画像データPの正当性を確認する画像検証装置20について説明する。

【0186】

図23は、第7の実施例の処理手順の一例を説明するフローチャートである。以下、図23を用いて、画像検証装置20がデジタル画像データPを検証する手順を説明する。

【0187】

ステップS2301において、外部I/F部301は、画像入力装置10が生成したデジタル画像データPとそれに対応するデジタル署名データhとを入力し、それらを画像検証装置20の作業用メモリ302に格納する。ここで、デジタル画像データPは、例えば、JPEG方式で高能率符号化されている（以下、デジタル画像データPを単にJPEGデータと称する）。

【0188】

ステップS2302において、操作部306は、ユーザの操作入力に基づき、どのJPEGデータの正当性を検証するか否かを選択する。検証が指示された場

合、制御／演算部303はステップS2303を実行する。

【0189】

ステップS2303において、制御／演算部303は、メモリ313から秘密情報Sを読み出す。ここで、この秘密情報Sは、第1の実施例の画像入力装置10と本実施例の画像検証装置20との間で秘密に共有する情報である。従って、本実施例の秘密情報Sは、第1の実施例と同様に“1111111”である。尚、この秘密情報Sは、読み出し専用の記録媒体等の中に保存され、外部に出力できないように管理されている。

【0190】

ステップS2304において、制御／演算部303（に含まれる演算回路312）は、秘密情報SとJPEGデータとを用いて、第1の実施例のステップS405と同様の演算を行う。つまり、JPEGデータの最上位バイトと秘密情報Sとを、ビット毎に排他的論理和演算する。

【0191】

ステップS2305において、制御／演算部303（に含まれる演算回路312）は、ステップS2304の演算結果をハッシュ関数で演算する。ここでは、第1の実施例と同様のハッシュ関数を使用して、ステップS406と同様の処理を行う。

【0192】

ステップS2306において、制御／演算部303（に含まれる演算回路312）は、ステップS2305の演算結果と選択されたJPEGデータのデジタル署名データhとを比較する。比較の結果、これらのデータが一致した場合には、JPEGデータを正当なものと判断し、一致しなかった場合には、JPEGデータに何らかの不正な処理（即ち、JPEGデータに対する修正、改竄、偽造、合成等の改変処理）が行われたものと判断する。

【0193】

ステップS2307において、表示部304は、ステップS2306の比較結果が一致した場合、選択したJPEGデータが正常で、不正な処理の施されていないことを示す表示画像或いはメッセージを表示する。又、この比較結果が一致

しなかった場合、不正な処理を示す警告画像或いは警告メッセージを表示する。これにより、ユーザは、選択した J P E G データの正当性を視覚的に分かり易く認識することができる。

【0194】

尚、図23に示す一連の処理手順を制御するプログラムは、ROM305に格納されている。このプログラムは、制御／演算部303（に含まれる制御回路312）によって読み出され、所望の画像の検証を指示する毎に起動する。

【0195】

以上の手順により、選択された J P E G データの正当性が確認されなかった場合、制御回路310は各処理回路を制御して該 J P E G データを廃棄する。

【0196】

以上説明したように、第7の実施例では、第1の実施例の画像入力装置10にて撮像され、高能率符号化されたデジタル画像データPの正当性を、従来のシステムに比べて簡単な構成で認識することができる。又、従来のシステムに比べて安価に構成することも、処理速度を高速化することもできる。

【0197】

（第8の実施例）

第8の実施例では、第2の実施例の画像入力装置10が生成したデジタル署名データhを用いて、デジタル画像データPの正当性を確認する画像検証装置20について説明する。

【0198】

図24は、第8の実施例の処理手順の一例を説明するフローチャートである。以下、図24を用いて、画像検証装置20がデジタル画像データPを検証する手順を説明する。

【0199】

ステップS2401、S2402の処理は、上述の第7の実施例のステップS2301、S2302と同様の処理としてその説明を省略する。

【0200】

ステップS2403において、制御／演算部303（に含まれる乱数発生回路

) は、ビット長mの乱数R（即ち、秘密情報S）を生成する。乱数Rを生成するためのプログラムは、ROM305に格納されている。このプログラムは、第2の実施例の画像入力装置10の保持するプログラムと同一であり、乱数Rは、第2の実施例の乱数Rと同一である。尚、このプログラム及び乱数Rは、外部に出力できないように管理されている。

【0201】

ステップS2404において、制御／演算部303（に含まれる演算回路312）は、図7に示すように、選択されたJPEGデータを128ビットのブロックD_i（i=1～n）に分割する。データ量が128ビットにならないブロックについては、“000…000”をパディングする。尚、ステップS2404の処理は、第2の実施例のステップS605と同様の処理である。

【0202】

ステップS2405において、制御／演算部303（に含まれる演算回路312）は、乱数Rとn個のブロックとを用いて、第2の実施例のステップS606と同様の演算を行う。つまり、乱数RのビットR_iとブロックD_iの最下位ビットとの間の排他的論理和演算を、i=1～nとなるまで繰り返す。

【0203】

ステップS2406において、制御／演算部303（に含まれる演算回路312）は、ステップS2405の演算結果に対してハッシュ関数演算を行う。ここでは、第2の実施例と同様のハッシュ関数を使用して、ステップS607と同様の処理を行う。

【0204】

ステップS2407において、制御／演算部303（に含まれる演算回路312）は、ステップS2406の演算結果と選択されたJPEGデータのディジタル署名データhとを比較する。比較の結果、これらのデータが一致した場合には、JPEGデータを正当なものと判断し、一致しなかった場合には、JPEGデータに何らかの不正な処理（即ち、JPEGデータに対する修正、改竄、偽造、合成等の改変処理）が行われたものと判断する。

【0205】

ステップS2408において、表示部304は、ステップS2407の比較結果を画像或いはメッセージで表示する。これにより、ユーザは、選択したJPEGデータの正当性を視覚的に分かり易く認識することができる。

【0206】

尚、図24に示す一連の処理手順を制御するプログラムは、ROM305に格納されている。このプログラムは、制御／演算部303（に含まれる制御回路312）によって読み出され、所望の画像の検証を指示する毎に起動する。

【0207】

以上の手順により、選択されたJPEGデータの正当性が確認されなかった場合、制御回路310は各処理回路を制御して該JPEGデータを廃棄する。

【0208】

以上説明したように、第8の実施例では、第2の実施例の画像入力装置10にて撮像され、高能率符号化されたデジタル画像データPの正当性を、従来のシステムに比べて簡単な構成で認識することができる。又、従来のシステムに比べて安価に構成することも、処理速度を高速化することもできる。

【0209】

（第9の実施例）

第9の実施例では、第3の実施例の画像入力装置10が生成したデジタル署名データhを用いて、デジタル画像データPの正当性を確認する画像検証装置20について説明する。

【0210】

図25は、第9の実施例の処理手順の一例を説明するフローチャートである。以下、図25を用いて、画像検証装置20がデジタル画像データPを検証する手順を説明する。

【0211】

ステップS2501、S2502の処理は、上述の第7の実施例のステップS2301、S2302と同様の処理としてその説明を省略する。

【0212】

ステップS2503において、制御／演算部303は、メモリ313から秘密

情報Sを読み出す。ここで、この秘密情報Sは、第3の実施例の画像入力装置10と本実施例の画像検証装置20との間で共有する情報である。従って、本実施例の秘密情報Sは、第3の実施例と同様に“11111111”である。尚、この秘密情報は、読み出し専用の記録媒体等の中に保存され、外部に出力できないように管理されている。

【0213】

ステップS2504において、制御／演算部303（に含まれる演算回路312）は、第3の実施例のステップS1405と同様に、選択されたJPEGデータを共通鍵暗号方式で暗号化する。

【0214】

ステップS2505において、制御／演算部303（に含まれる演算回路312）は、ステップS2504にて生成された暗号データから特定のビット列を抽出する。例えば、第3の実施例と同様に、上述の暗号データの下位128ビットを抽出する。

【0215】

ステップS2506において、制御／演算部303（に含まれる演算回路312）は、ステップS2505の抽出結果と選択されたJPEGデータのデジタル署名データhとを比較する。比較の結果、これらのデータが一致した場合には、JPEGデータを正当なものと判断し、一致しなかった場合には、JPEGデータに何らかの不正な処理（即ち、JPEGデータに対する修正、改竄、偽造、合成等の改変処理）が行われたものと判断する。

【0216】

ステップS2507において、表示部304は、ステップS2506の比較結果を画像或いはメッセージで表示する。これにより、ユーザは、選択したJPEGデータの正当性を視覚的に分かり易く認識することができる。

【0217】

尚、図25に示す一連の処理手順を制御するプログラムは、ROM305に格納されている。このプログラムは、制御／演算部303（に含まれる制御回路312）によって読み出され、所望の画像の検証を指示する毎に起動する。

【0218】

以上の手順により、選択されたJPGデータの正当性が確認されなかった場合、制御回路310は各処理回路を制御して該JPGデータを廃棄する。

【0219】

以上説明したように、第9の実施例では、第3の実施例の画像入力装置10にて撮像され、高能率符号化されたデジタル画像データPの正当性を、従来のシステムに比べて簡単な構成で認識することができる。又、従来のシステムに比べて安価に構成することも、処理速度を高速化することもできる。

【0220】**(第10の実施例)**

第10の実施例では、第4の実施例の画像入力装置10が生成したデジタル署名データhを用いて、デジタル画像データPの正当性を確認する画像検証装置20について説明する。

【0221】

図26は、第10の実施例の処理手順の一例を説明するフローチャートである。以下、図26を用いて、画像検証装置20がデジタル画像データPを検証する手順を説明する。

【0222】

ステップS2601、S2602の処理は、上述の第7の実施例のステップS2301、S2302と同様の処理としてその説明を省略する。

【0223】

ステップS2603～S2605の処理は、上述の第8の実施例のステップS2403～S2405と同様の処理としてその説明を省略する。

【0224】

ステップS2606において、制御／演算部303（に含まれる演算回路312）は、第4の実施例のステップS1907と同様に、選択されたJPGデータを共通鍵暗号方式で暗号化する。

【0225】

ステップS2607において、制御／演算部303（に含まれる演算回路31

2) は、ステップS2606にて生成された暗号データから特定のビット列を抽出する。例えば、第3の実施例と同様に、上述の暗号データの下位128ビットを抽出する。

【0226】

ステップS2608において、制御／演算部303（に含まれる演算回路312）は、ステップS2607の抽出結果と選択されたJPEGデータのデジタル署名データhとを比較する。比較の結果、これらのデータが一致した場合には、JPEGデータを正当なものと判断し、一致しなかった場合には、JPEGデータに何らかの不正な処理（即ち、JPEGデータに対する修正、改竄、偽造、合成等の改変処理）が行われたものと判断する。

【0227】

ステップS2609において、表示部304は、ステップS2608の比較結果を画像或いはメッセージで表示する。これにより、ユーザは、選択したJPEGデータの正当性を視覚的に分かり易く認識することができる。

【0228】

尚、図26に示す一連の処理手順を制御するプログラムは、ROM305に格納されている。このプログラムは、制御／演算部303（に含まれる制御回路312）によって読み出され、所望の画像の検証を指示する毎に起動する。

【0229】

以上の手順により、選択されたJPEGデータの正当性が確認されなかった場合、制御回路310は各処理回路を制御して該JPEGデータを廃棄する。

【0230】

以上説明したように、第10の実施例では、第4の実施例の画像入力装置10にて撮像され、高能率符号化されたデジタル画像データPの正当性を、従来のシステムに比べて簡単な構成で認識することができる。又、従来のシステムに比べて安価に構成することも、処理速度を高速化することもできる。

【0231】

（第11の実施例）

第11の実施例では、第5の実施例の画像入力装置10が生成したデジタル

署名データhを用いて、ディジタル画像データPの正当性を確認する画像検証装置20について説明する。

【0232】

図27は、第11の実施例の処理手順の一例を説明するフローチャートである。以下、図27を用いて、画像検証装置20がディジタル画像データPを検証する手順を説明する。

【0233】

ステップS2701において、画像検証装置20の制御/演算処理部303は、外部I/F部301に外部装置40が接続されているか否かを検出する。

【0234】

ステップS2702において、画像検証装置20と外部装置40とは、相互認証を行い、互いに正当なものであるかどうかをチェックする。

【0235】

ステップS2703、S2704の処理は、上述の第7の実施例のステップS2301、S2302と同様の処理としてその説明を省略する。

【0236】

ステップS2705において、制御/演算部303は、外部I/F部301を介して入力された外部装置40に固有の秘密情報Sをメモリ313に格納し、管理する。

【0237】

ステップS2706において、制御/演算部303（に含まれる演算回路312）は、秘密情報SとJPEGデータとを用いて、予め定められた規則に基づく所定の演算を行う。ここで、演算回路312は、第7の実施例のステップS2304と同様の演算を行う。

【0238】

ステップS2707において、制御/演算部303（に含まれる演算回路312）は、ステップS2706の演算結果をハッシュ関数で演算する。ここで、演算回路312は、第7の実施例のステップS2305と同様の演算を行う。

【0239】

ステップS2708において、制御／演算部303（に含まれる演算回路312）は、ステップS2707の演算結果と選択されたJPEGデータのデジタル署名データhとを比較する。比較の結果、これらのデータが一致した場合には、JPEGデータを正当なものと判断し、一致しなかった場合には、JPEGデータに何らかの不正な処理（即ち、JPEGデータに対する修正、改竄、偽造、合成等の改変処理）が行われたものと判断する。

【0240】

ステップS2709において、表示部304は、ステップS2708の比較結果を画像或いはメッセージで表示する。これにより、ユーザは、選択したJPEGデータの正当性を視覚的に分かり易く認識することができる。

【0241】

尚、図27に示す一連の処理手順を制御するプログラムは、ROM305に格納されている。このプログラムは、制御／演算部303（に含まれる制御回路312）によって読み出され、所望の画像の検証を指示する毎に起動する。

【0242】

以上の手順により、選択されたJPEGデータの正当性が確認されなかった場合、制御回路310は各処理回路を制御して該JPEGデータを廃棄する。

【0243】

以上説明したように、第11の実施例では、第5の実施例の画像入力装置10にて撮像され、高能率符号化されたデジタル画像データPの正当性を、従来のシステムに比べて簡単な構成で認識することができる。又、従来のシステムに比べて安価に構成することも、処理速度を高速化することもできる。更に、デジタル署名データhを用いて、デジタル画像データがどの外部機器によって撮像されたものか、或いはどのユーザにて撮像されたものかを特定することもできる。

【0244】

（第12の実施例）

第12の実施例では、第6の実施例の画像入力装置10が生成したデジタル署名データhを用いて、デジタル画像データPの正当性を確認する画像検証装

置20について説明する。

【0245】

図27を用いて、第12の実施例の処理手順の一例を説明する。

【0246】

ステップS2701～S2704の処理は、上述の第11の実施例と同様の処理としてその説明を省略する。

【0247】

ステップS2705において、制御／演算部303は、画像入力装置10と供給する秘密情報S1をメモリ313から読み出し、外部装置40に固有の秘密情報S2を外部I／F部301を介して入力する。そして、第6の実施例と同様に、これらの秘密情報S1、S2を結合し、新しい秘密情報Sを生成する。

【0248】

ステップS2706において、制御／演算部303（に含まれる演算回路312）は、秘密情報SとJPEGデータとを用いて、予め定められた規則に基づく所定の演算を行う。ここで、演算回路312は、第7の実施例のステップS2304と同様の演算処理を行う。

【0249】

ステップS2707において、制御／演算部303（に含まれる演算回路312）は、ステップS2706の演算結果をハッシュ関数で演算する。ここで、演算回路312は、第7の実施例のステップS2305と同様の演算処理を行う。

【0250】

ステップS2708において、制御／演算部303（に含まれる演算回路312）は、ステップS2707の演算結果と選択されたJPEGデータのディジタル署名データhとを比較する。比較の結果、これらのデータが一致した場合には、JPEGデータを正当なものと判断し、一致しなかった場合には、JPEGデータに何らかの不正な処理（即ち、JPEGデータに対する修正、改竄、偽造、合成等の改変処理）が行われたものと判断する。

【0251】

ステップS2709において、表示部304は、ステップS2708の比較結

果を画像或いはメッセージで表示する。これにより、ユーザは、選択した J P E G データの正当性を視覚的に分かり易く認識することができる。

【0252】

尚、図 27 に示す一連の処理手順を制御するプログラムは、ROM305 に格納されている。このプログラムは、制御／演算部 303（に含まれる制御回路 312）によって読み出され、所望の画像の検証を指示する毎に起動する。

【0253】

以上の手順により、選択された J P E G データの正当性が確認されなかった場合、制御回路 310 は各処理回路を制御して該 J P E G データを廃棄する。

【0254】

以上説明したように、第 12 の実施例では、第 6 の実施例の画像入力装置 10 にて撮像され、高能率符号化されたデジタル画像データ P の正当性を、従来のシステムに比べて簡単な構成で認識することができる。又、従来のシステムに比べて安価に構成することも、処理速度を高速化することもできる。更に、上述のデジタル署名データ h を用いて、デジタル画像データがどの外部機器と接続された画像入力装置によって撮像されたものか、或いはどのユーザによって使用された画像入力装置にて撮像されたものかを特定することもできる。

【0255】

尚、本発明はその精神、又は主要な特徴から逸脱することなく、他の様々な形で実施することができる。

【0256】

例えば、第 1～第 6 の実施例では、画像入力装置 10 内においてデジタル署名データを生成したが、該デジタル署名データを画像入力装置 10 に接続された外部装置 40 にて生成することも可能である。このように構成した場合、各装置が互いの装置を認証した後、デジタル署名データの生成に必要な処理プログラム、高能率符号化されたデジタル画像データ等を画像入力装置 10 から外部装置 40 に送信し、デジタル署名データを生成する。

【0257】

又、第 1～第 6 の実施例では、デジタル署名データの生成に必要な演算処理

を画像入力装置10と外部装置40とに分散させ、各装置が共同してデジタル署名データを生成することも可能である。このように構成した場合、各装置が互いの装置を認証した後、デジタル署名データの生成に必要な処理プログラム、高能率符号化されたデジタル画像データ等の中で必要な部分のみを画像入力装置10から外部装置40に送信し、デジタル署名データを生成する。

【0258】

又、第7～第12の実施例では、画像検証装置20が外部入力されたデジタル画像データを用いてデジタル署名データを生成したが、該デジタル署名データを画像検証装置20に接続された外部装置40にて生成することも可能である。このように構成した場合、各装置が互いの装置を認証した後、デジタル署名データの生成に必要な処理プログラム、外部入力されたデジタル画像データ等を画像検証装置20から外部装置40に送信し、デジタル署名データを生成する。

【0259】

又、第7～第12の実施例では、デジタル署名データの生成に必要な演算処理を画像検証装置20と外部装置40とに分散させ、各装置が共同してデジタル署名データを生成することも可能である。このように構成した場合、各装置が互いの装置を認証した後、デジタル署名データの生成に必要な処理プログラム、外部入力されたデジタル画像データ等の中で必要な部分のみを画像検証装置20から外部装置40に送信し、デジタル署名データを生成する。

【0260】

又、第7～第12の実施例では、図23～図27に示す一連の処理手順を制御するプログラムは、所望の画像の検証を指示する毎に起動する構成として説明したが、所望の画像を外部入力することに自動的に起動するように構成してもよい。

【0261】

従って、前述の各実施例ではあらゆる点で単なる例示に過ぎず、限定的に解釈してはならない。

【0262】

【発明の効果】

以上のように、本発明によれば、デジタルデータの著作権を保護すると共に、そのデジタルデータに対する不正な処理を検出するための署名データを簡単な構成で、高速に生成することができる。又、その署名データを用いて、デジタルデータに対する不正な処理を簡単な構成で、高速且つ確実に検出することができる。

【0263】

又、本発明によれば、デジタルデータとそのデジタルデータを生成した機器の秘密情報とを用いて署名データを生成することにより、あるデジタルデータがどの機器によって生成されたかを特定することができる。

【0264】

又、本発明によれば、デジタルデータとそのデジタルデータを生成した機器の秘密情報とを用いて署名データを生成することにより、あるデジタルデータがどの機器によって生成されたかを特定することができる。

【0265】

又、本発明によれば、デジタルデータとそのデジタルデータを生成した機器に接続された外部機器の秘密情報とを用いて署名データを生成することにより、あるデジタルデータがどの外部機器と接続された機器或いはどのユーザによって使用された機器にて生成されたかを特定することもできる。

【0266】

又、本発明によれば、デジタルデータとそのデジタルデータを生成した機器の秘密情報とその機器に接続された外部機器の秘密情報とを用いて署名データを生成することにより、あるデジタルデータがどの外部機器と接続された機器或いはどのユーザによって使用された機器にて生成されたかを特定することもできる。

【図面の簡単な説明】

【図1】

本実施例のデジタル画像検証システムについて説明する図。

【図2】

本実施例の画像入力装置の基本構成について説明するブロック図。

【図3】

本実施例の画像検証装置の基本構成について説明するブロック図。

【図4】

第1の実施例の処理手順を説明するフローチャート。

【図5】

第1の実施例における所定の演算処理を説明する図。

【図6】

第2の実施例の処理手順を説明するフローチャート。

【図7】

第2の実施例におけるJPEGデータを表す図。

【図8】

第2の実施例における秘密情報を説明する図。

【図9】

第2の実施例における所定の演算処理を説明する図。

【図10】

第2の実施例におけるハッシュ関数演算の第1のモードを説明する図。

【図11】

第2の実施例におけるハッシュ関数演算の第2のモードを説明する図。

【図12】

第2の実施例におけるハッシュ関数演算の第3のモードを説明する図。

【図13】

第1～第3のモードにおける使用される初期値を説明する図。

【図14】

第3の実施例の処理手順を説明するフローチャート。

【図15】

第3の実施例における秘密情報を説明する図。

【図16】

第3の実施例におけるCBCモードを説明する図。

【図17】

第3の実施例におけるC F B モードを説明する図。

【図18】

第3の実施例におけるO F B モードを説明する図。

【図19】

第4の実施例の処理手順を説明するフローチャート。

【図20】

第4の実施例における秘密情報を説明する図。

【図21】

第5、第6の実施例の処理手順を説明するフローチャート。

【図22】

画像入力装置と外部装置とを説明する図。

【図23】

第7の実施例の処理手順を説明するフローチャート。

【図24】

第8の実施例の処理手順を説明するフローチャート。

【図25】

第9の実施例の処理手順を説明するフローチャート。

【図26】

第10の実施例の処理手順を説明するフローチャート。

【図27】

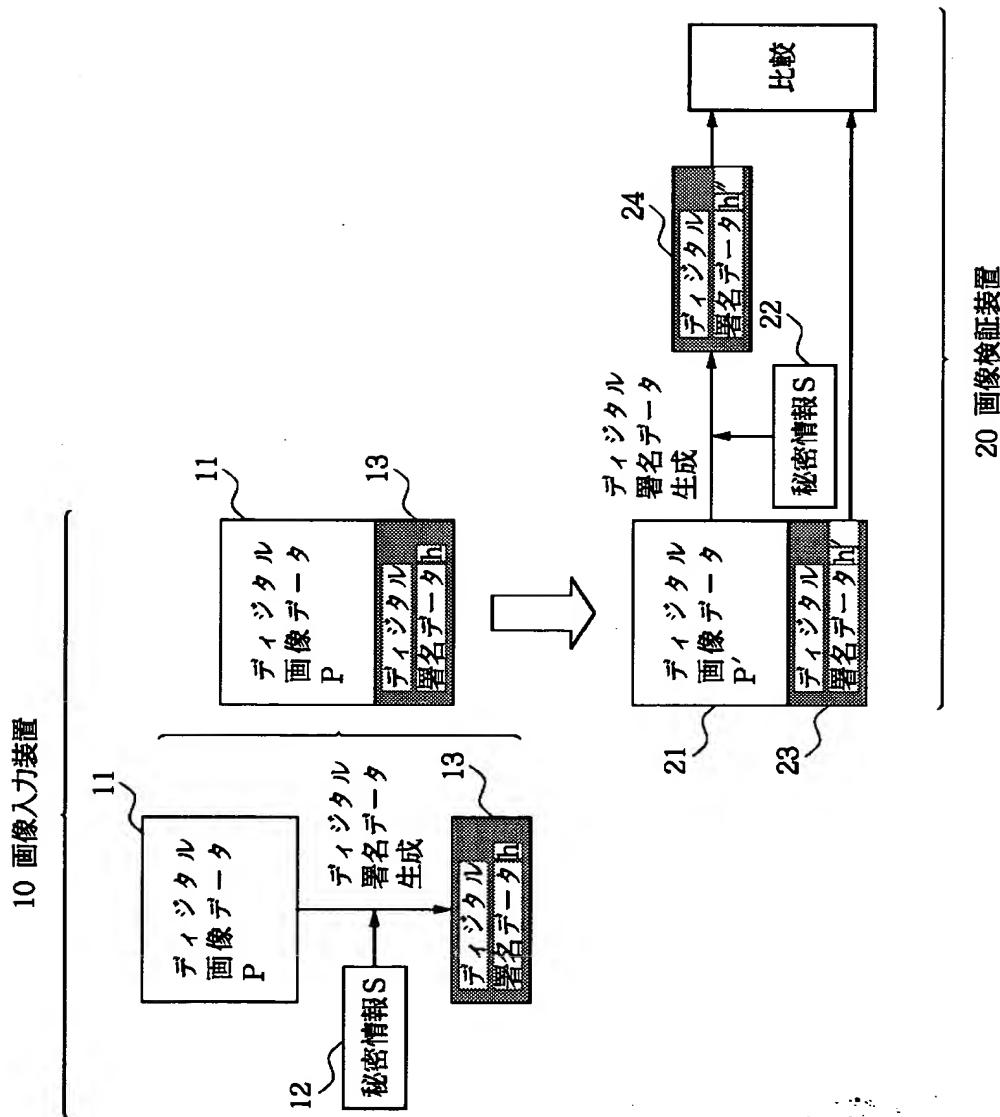
第11、第12の実施例の処理手順を説明するフローチャート。

【図28】

従来のシステムを説明する図。

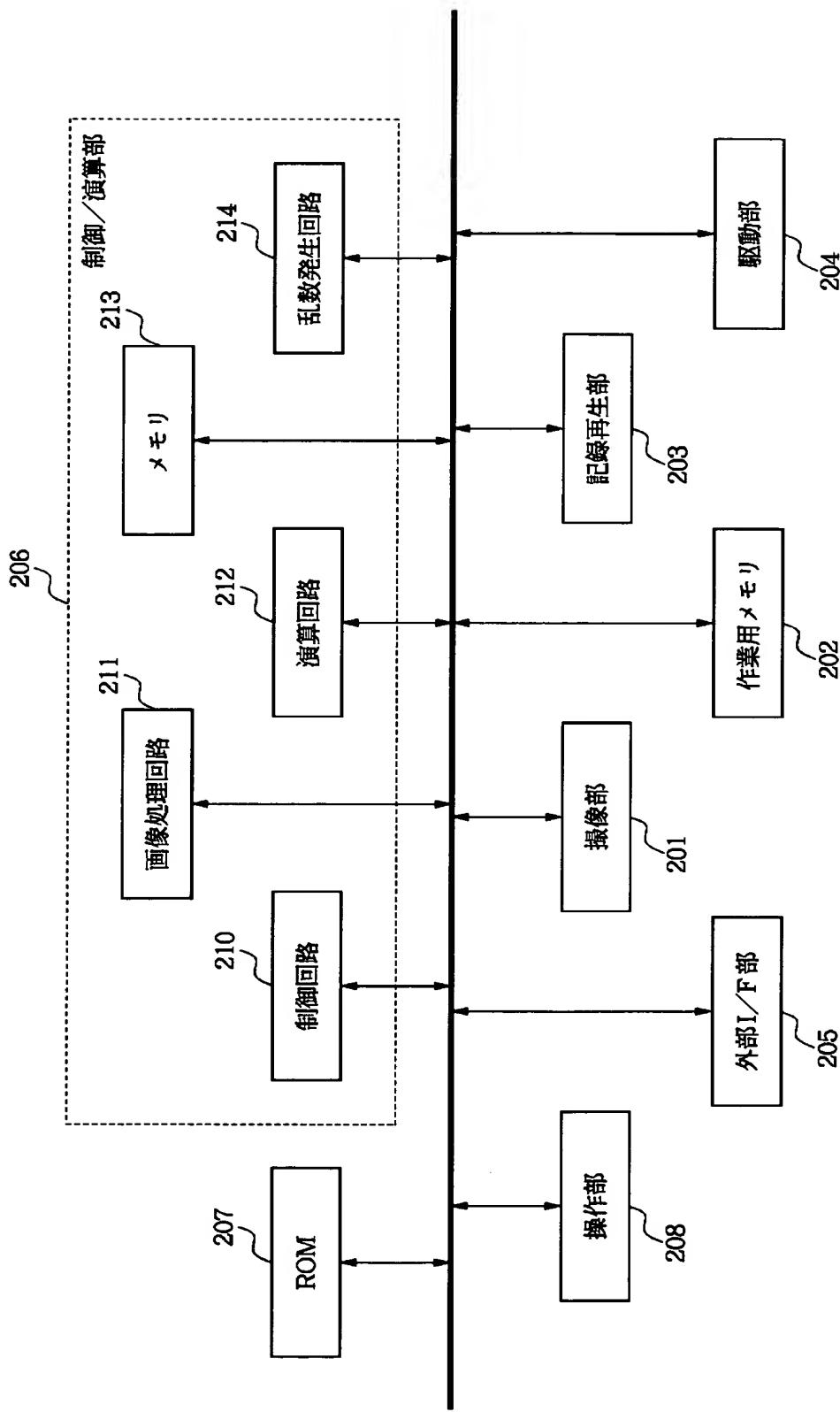
【書類名】 図面

【図1】

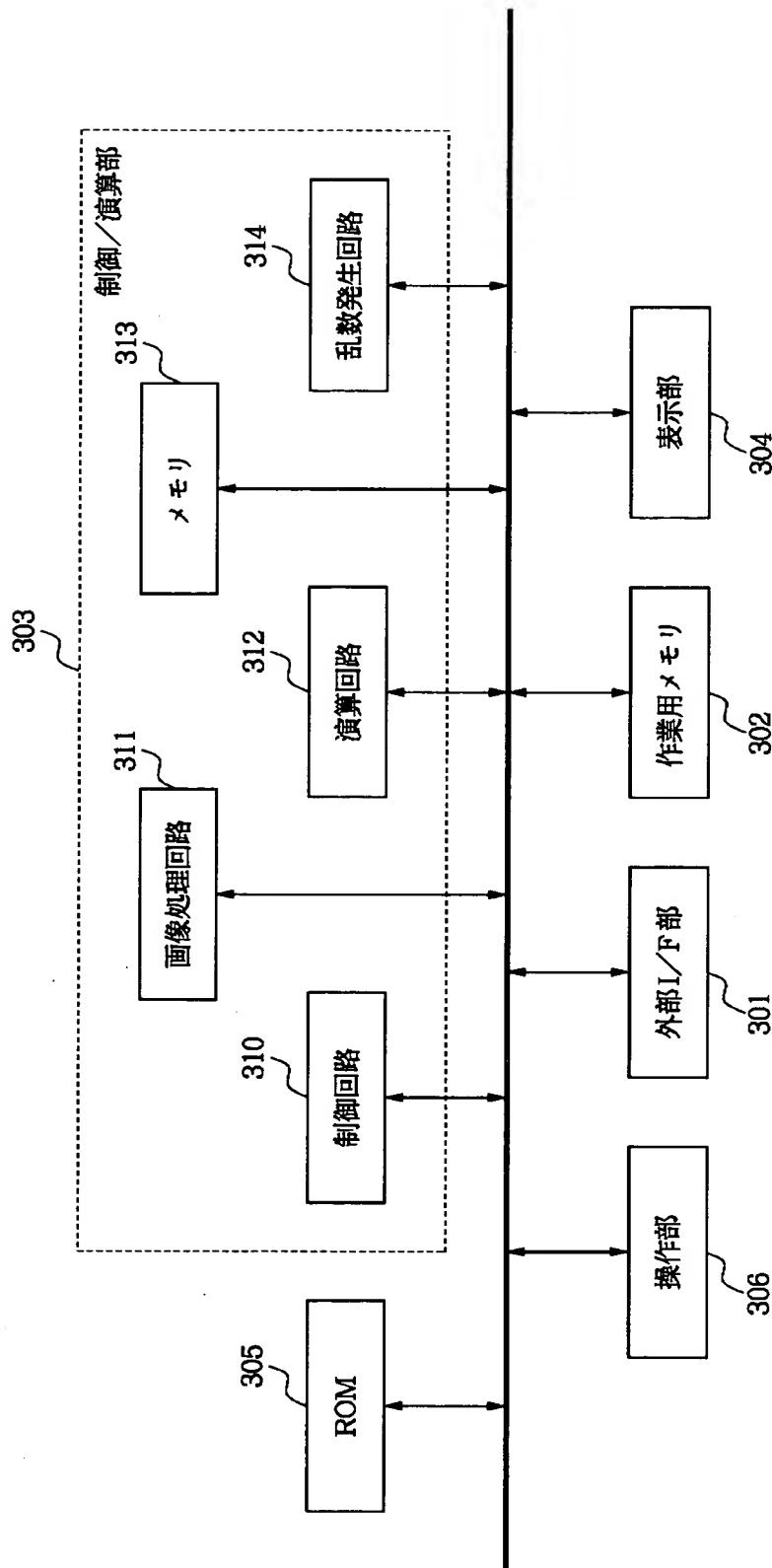


20 画像検証装置

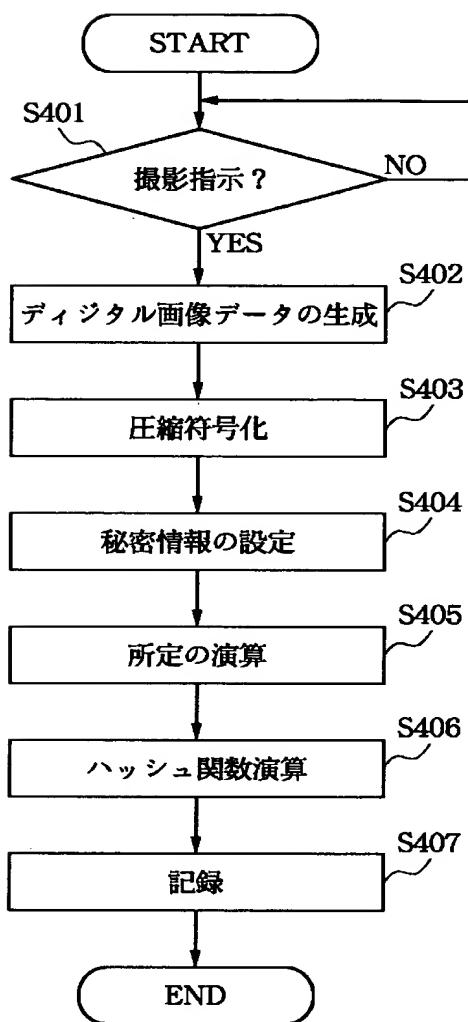
【図2】



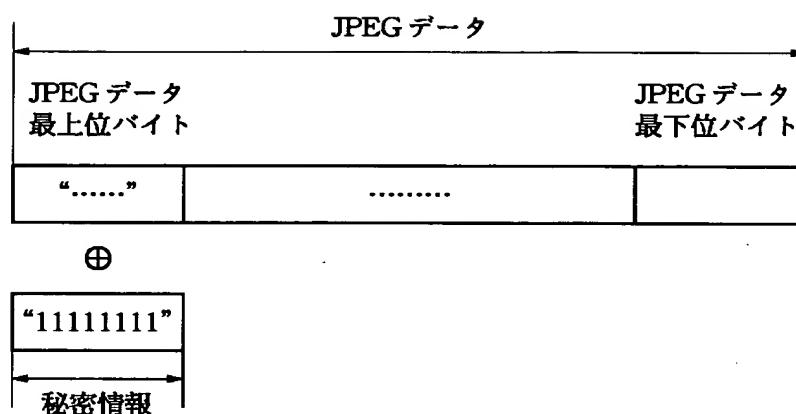
【図3】



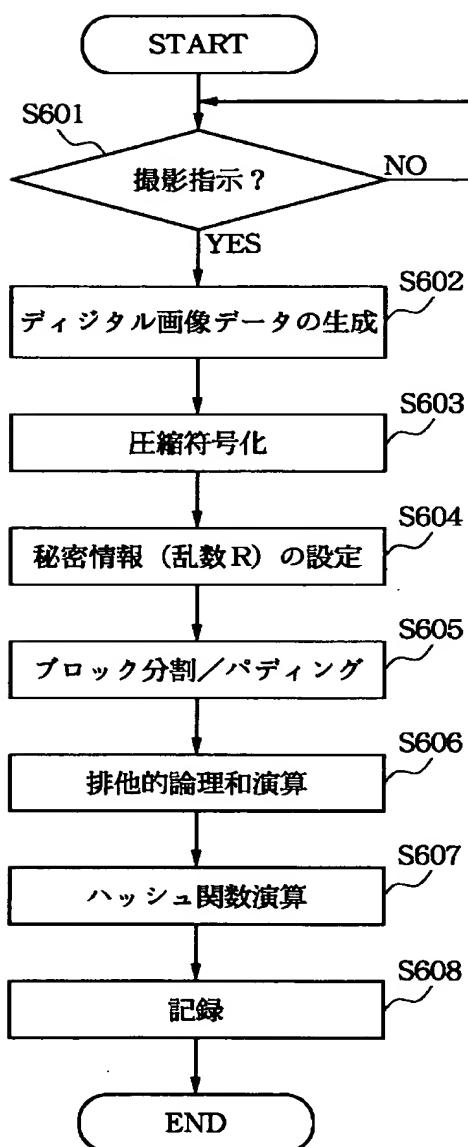
【図4】



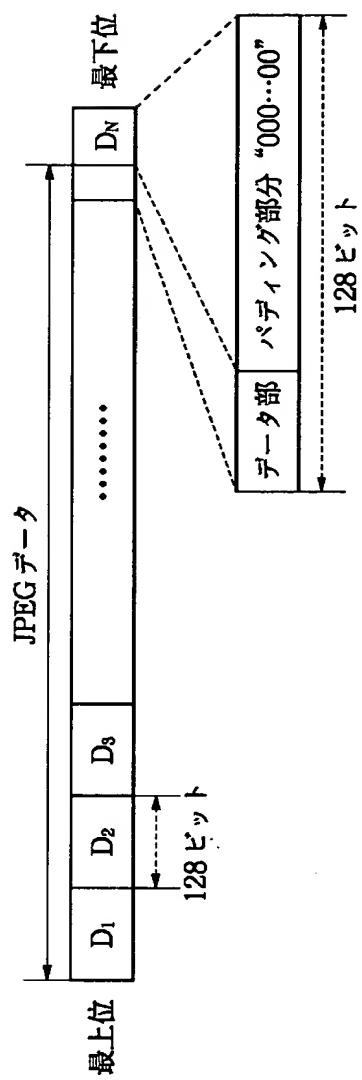
【図5】



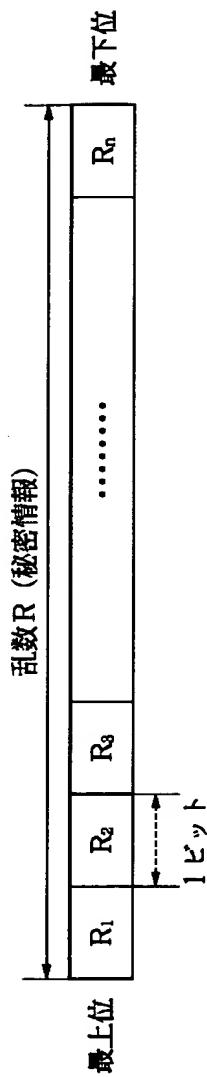
【図6】



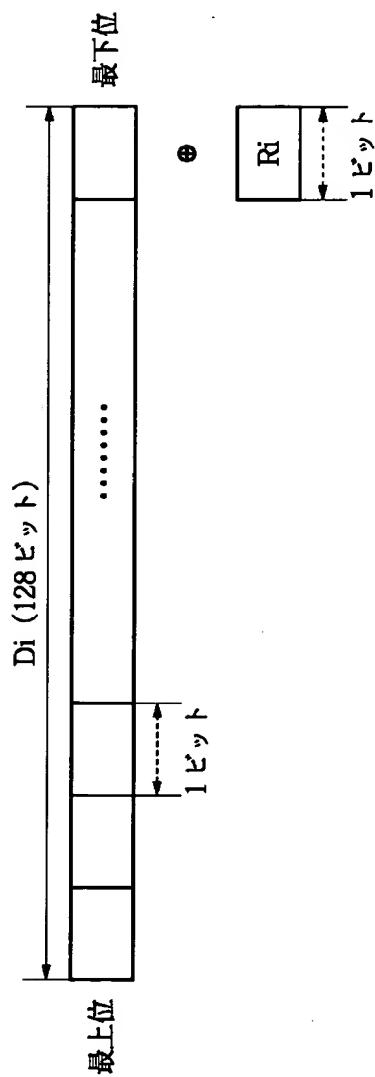
【図7】



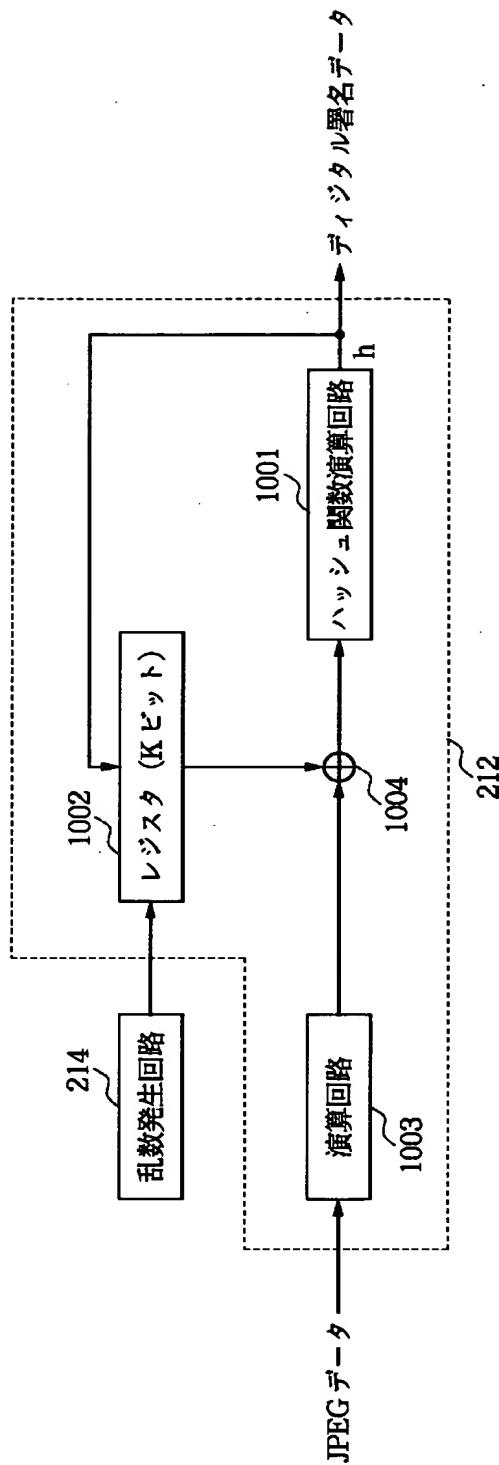
【図8】



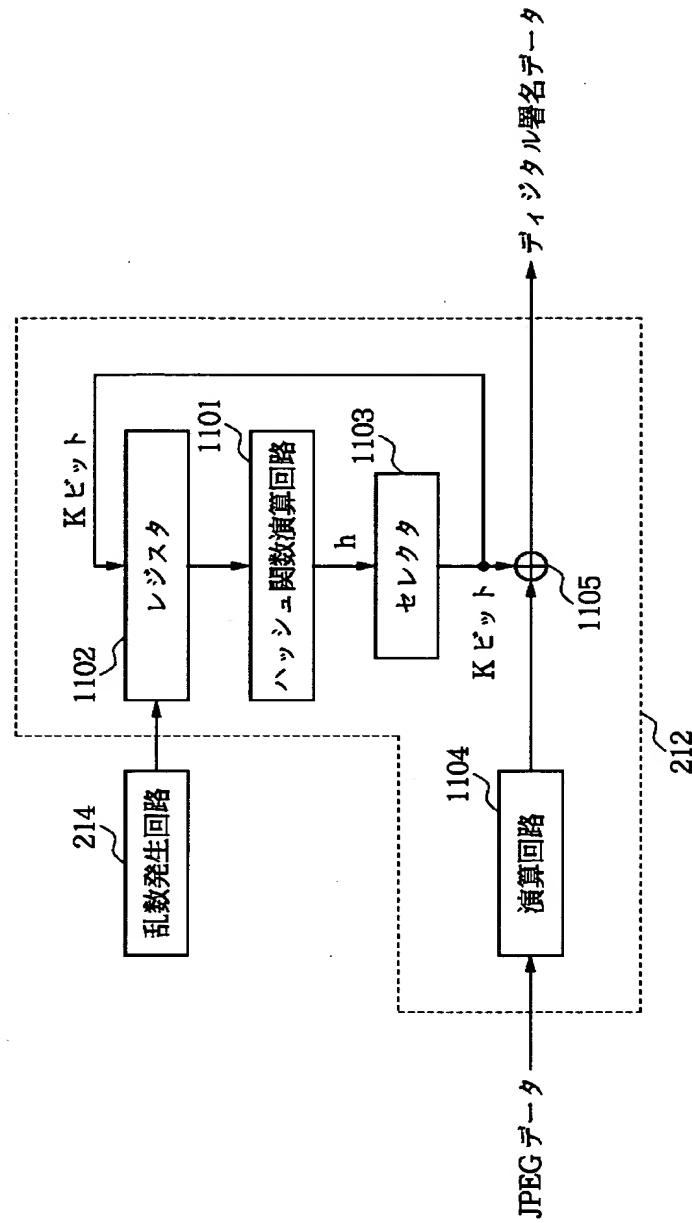
【図9】



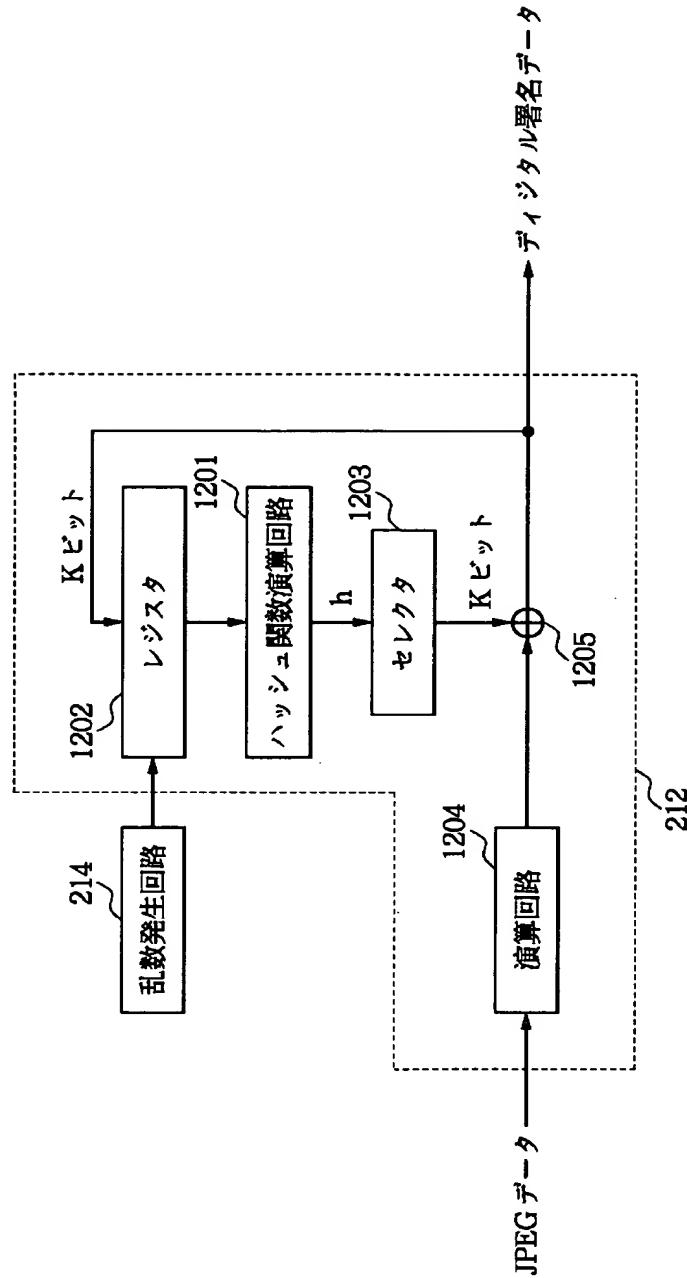
【図10】



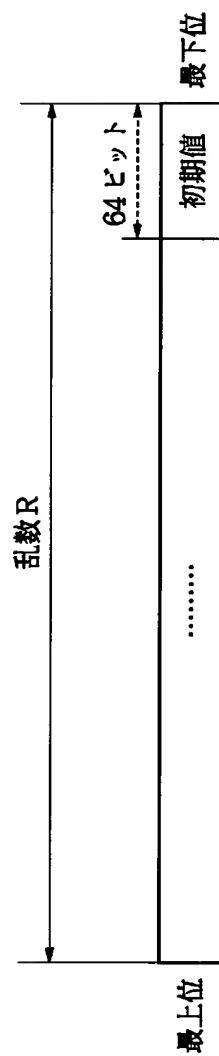
【図11】



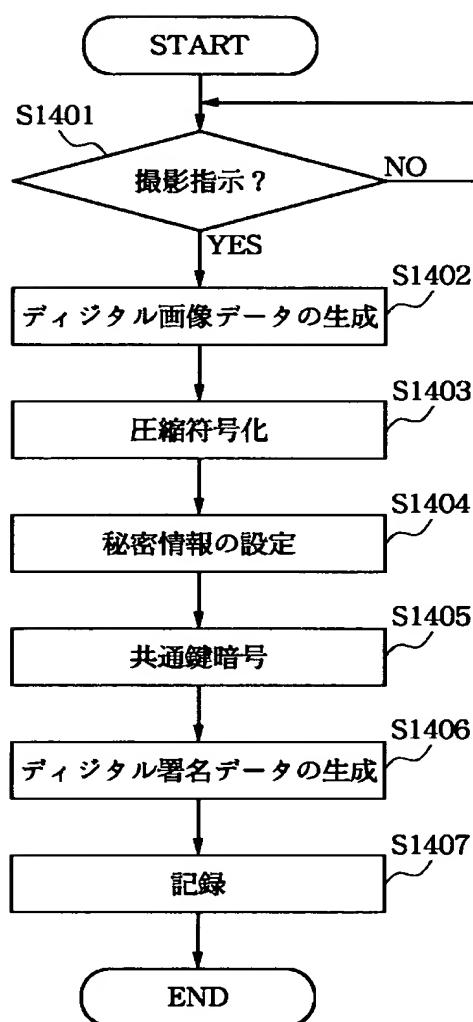
【図12】



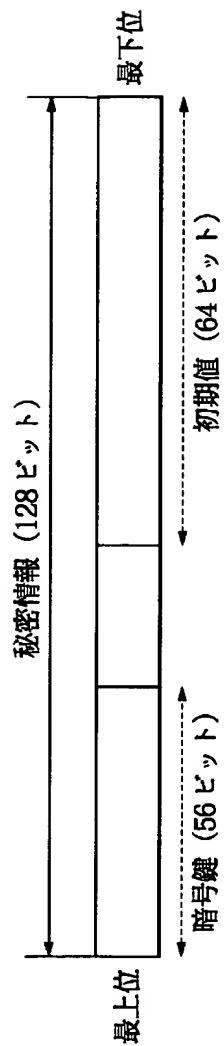
【図13】



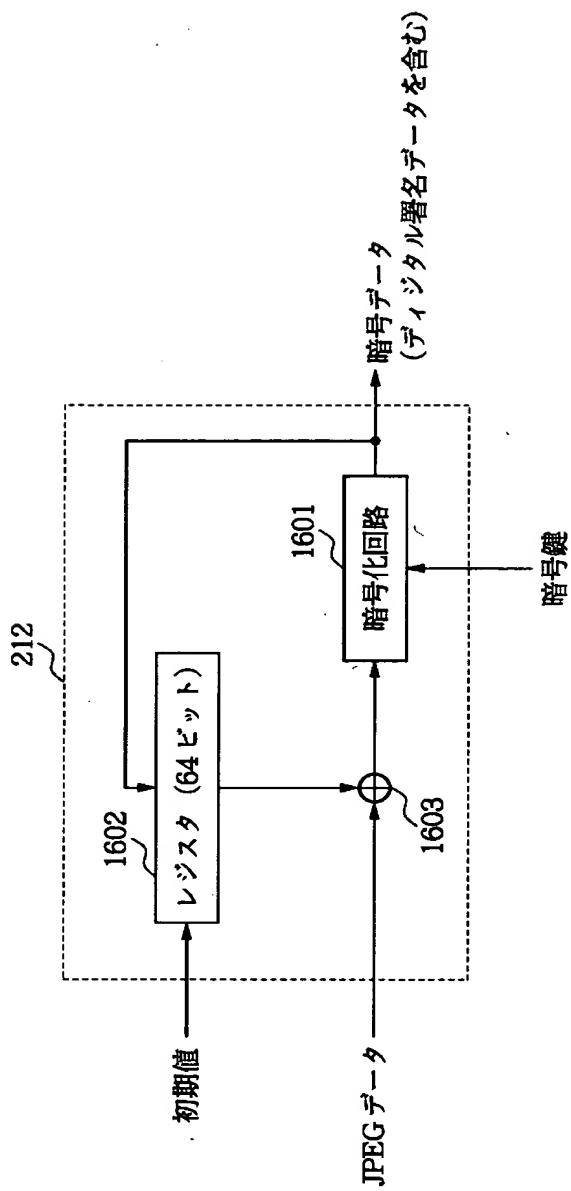
【図14】



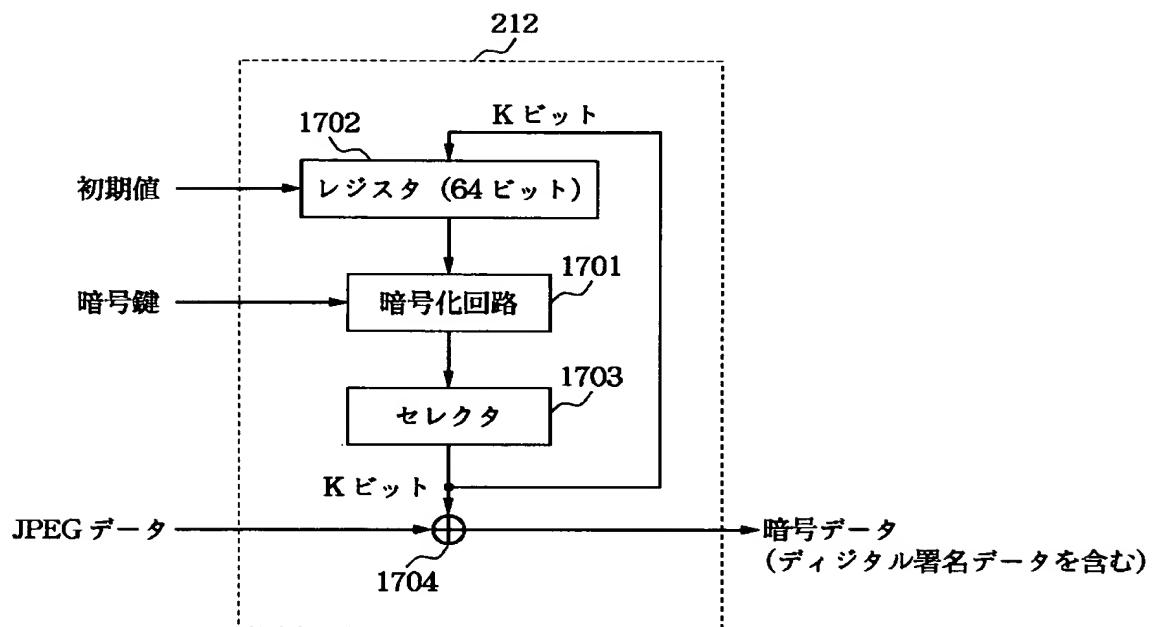
【図15】



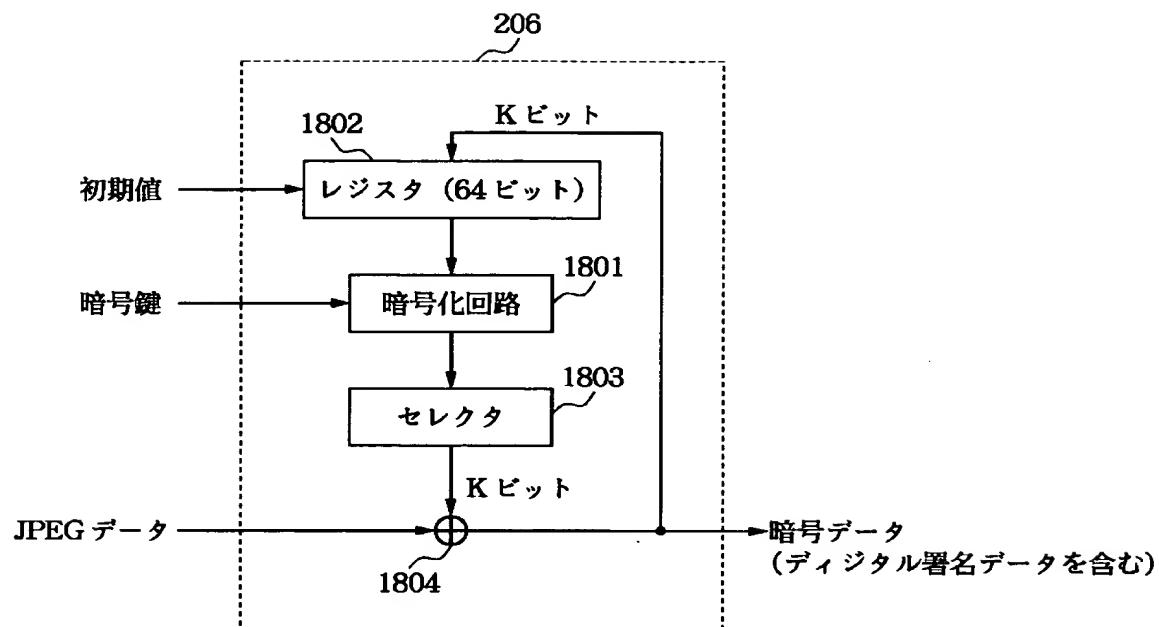
【図16】



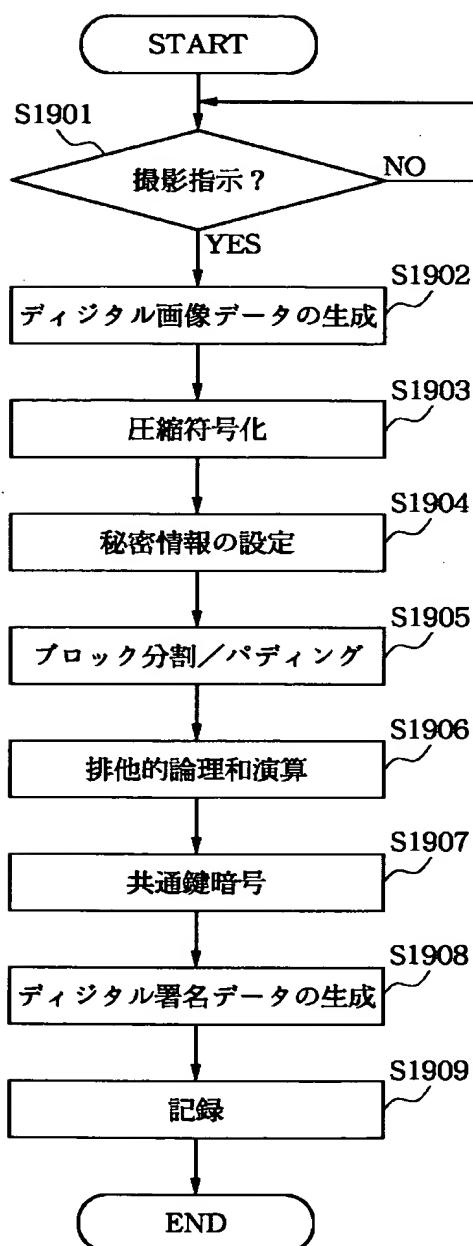
【図17】



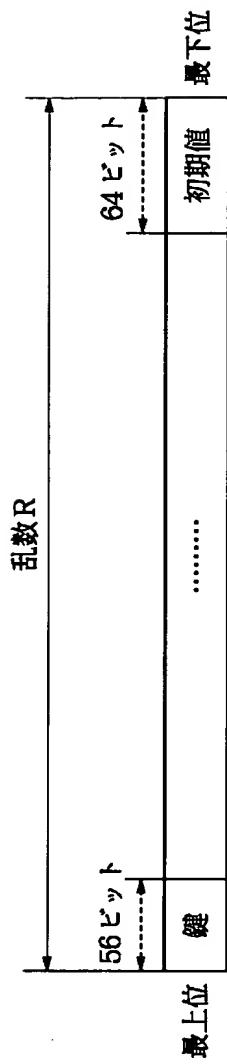
【図18】



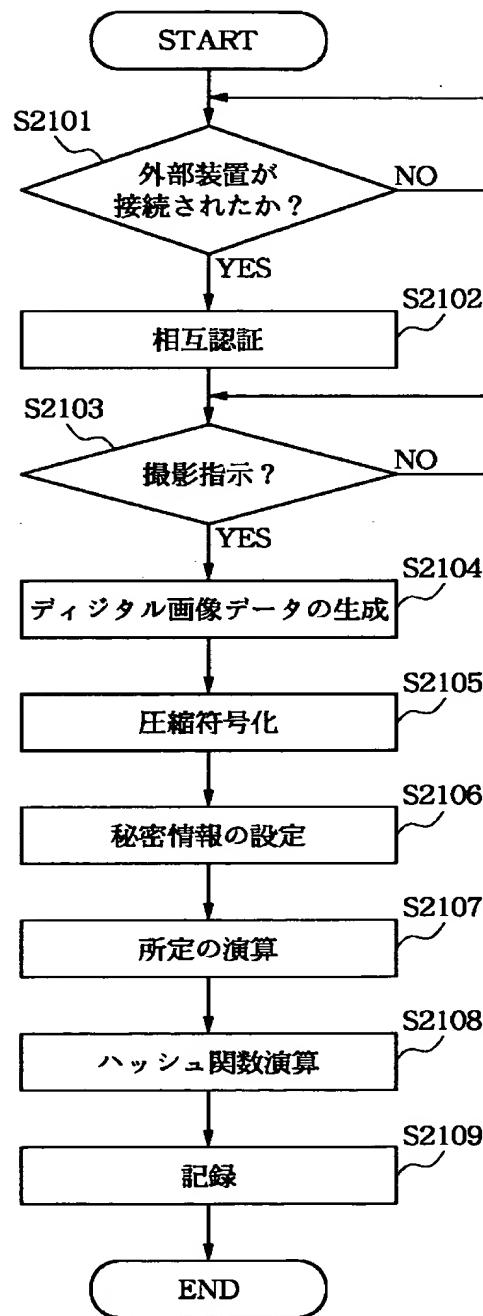
【図19】



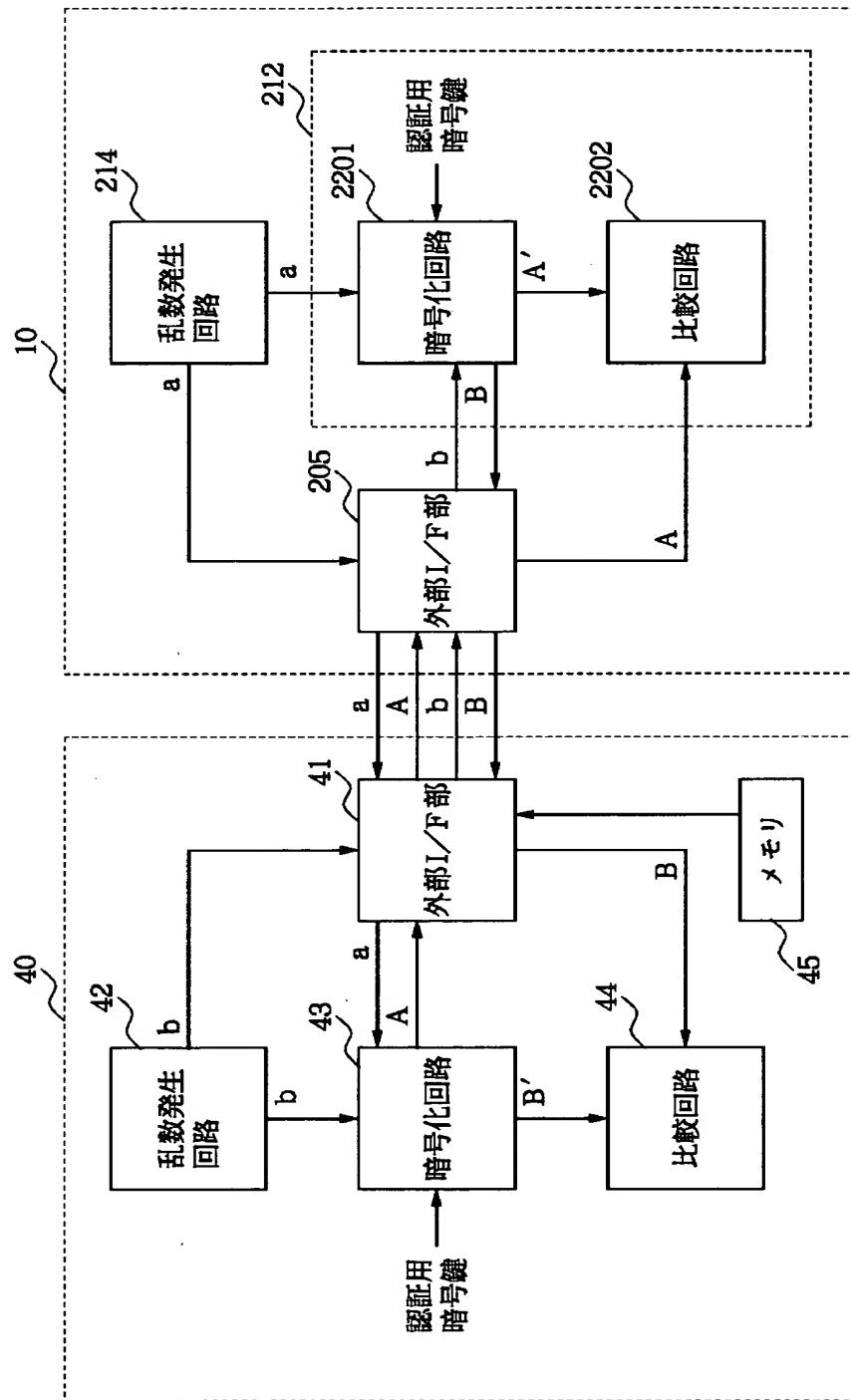
【図20】



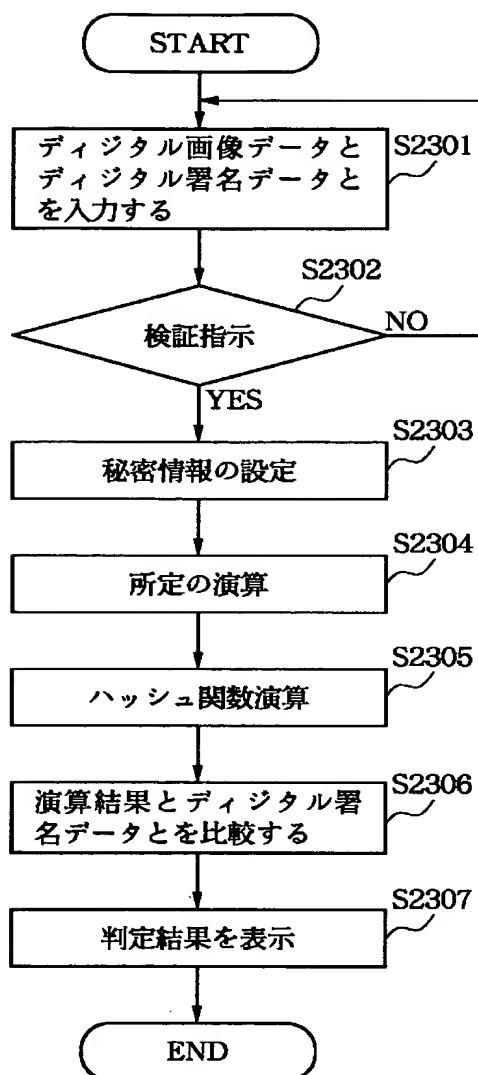
【図21】



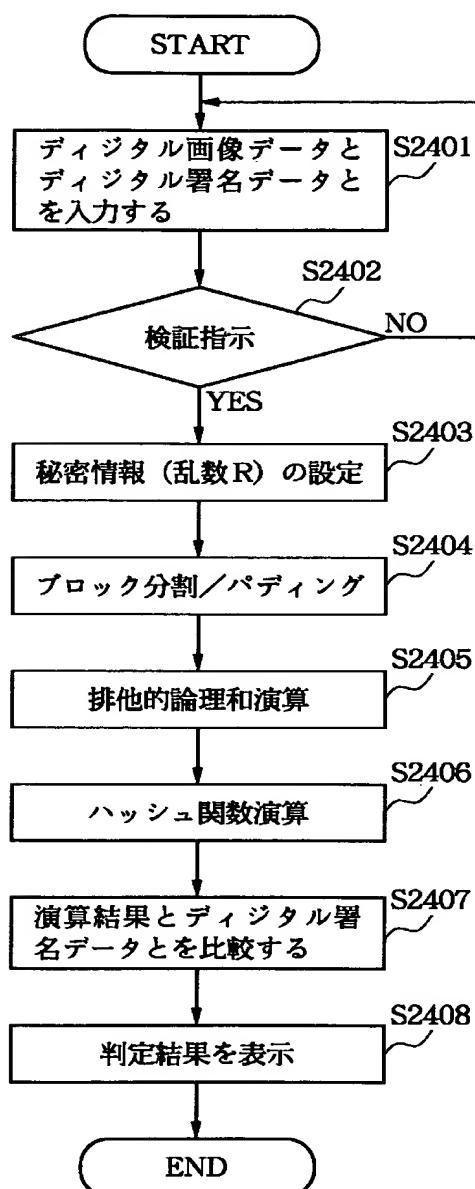
【図22】



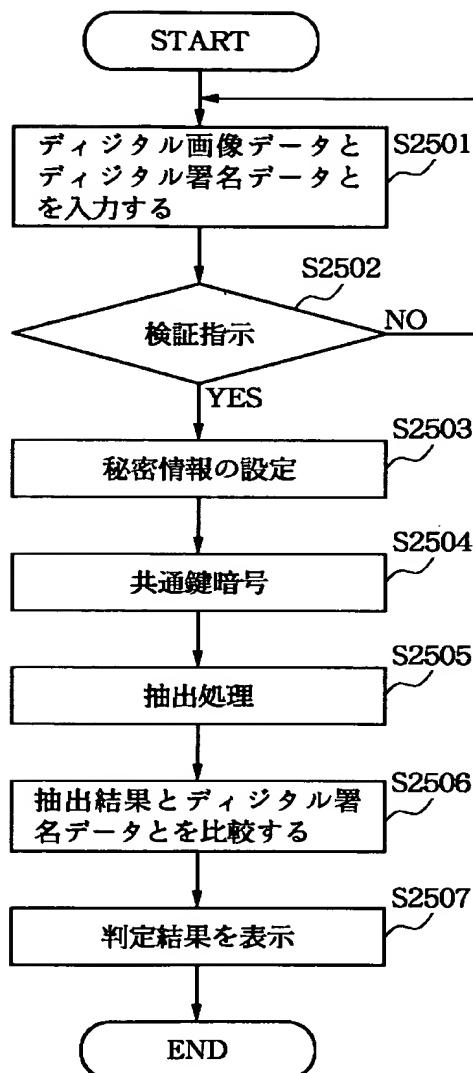
【図23】



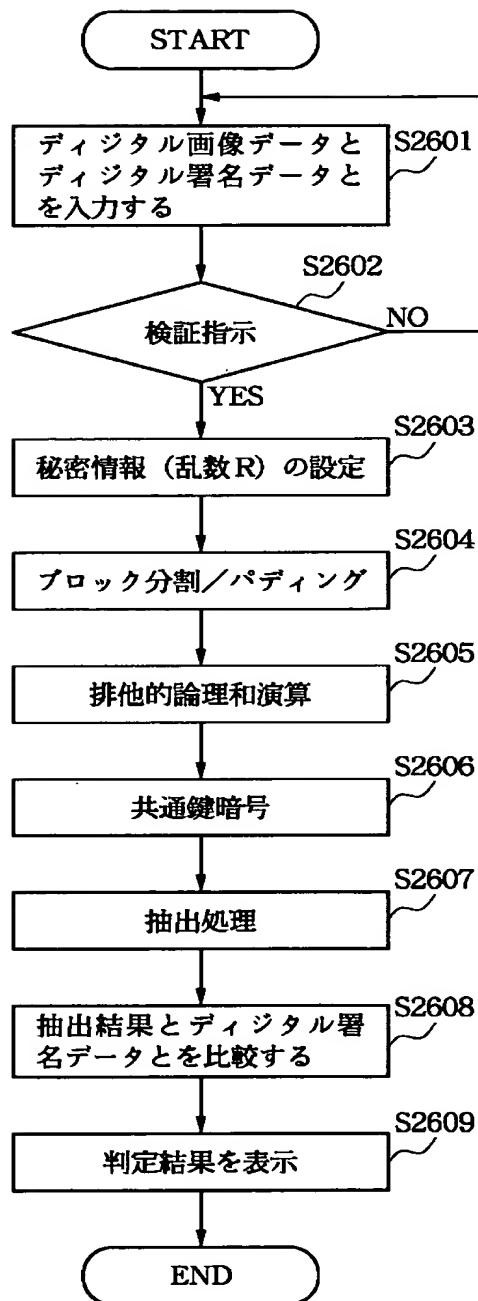
【図24】



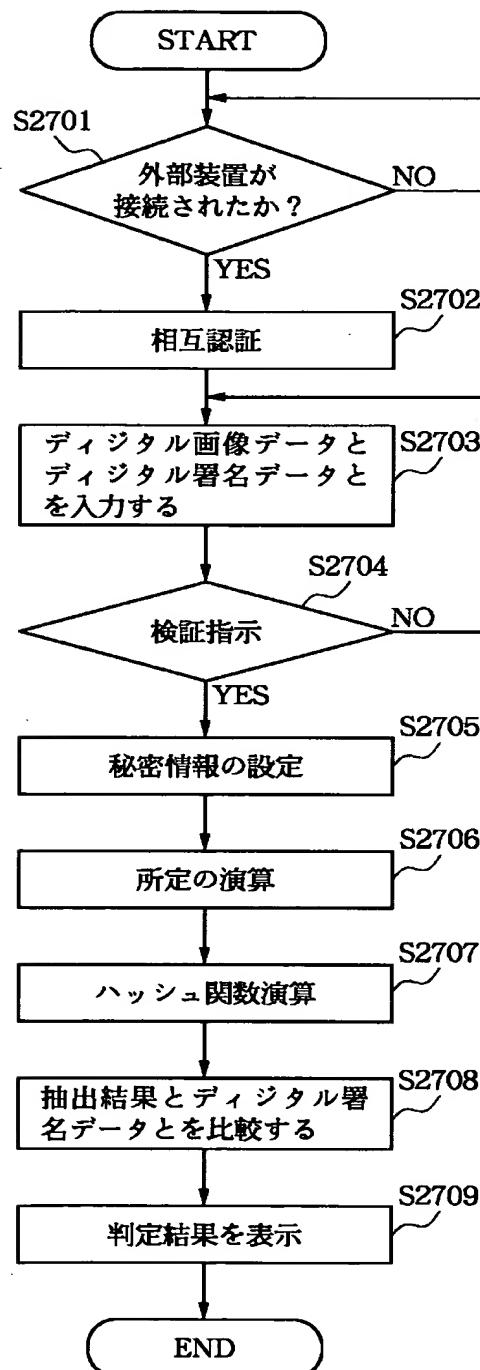
【図25】



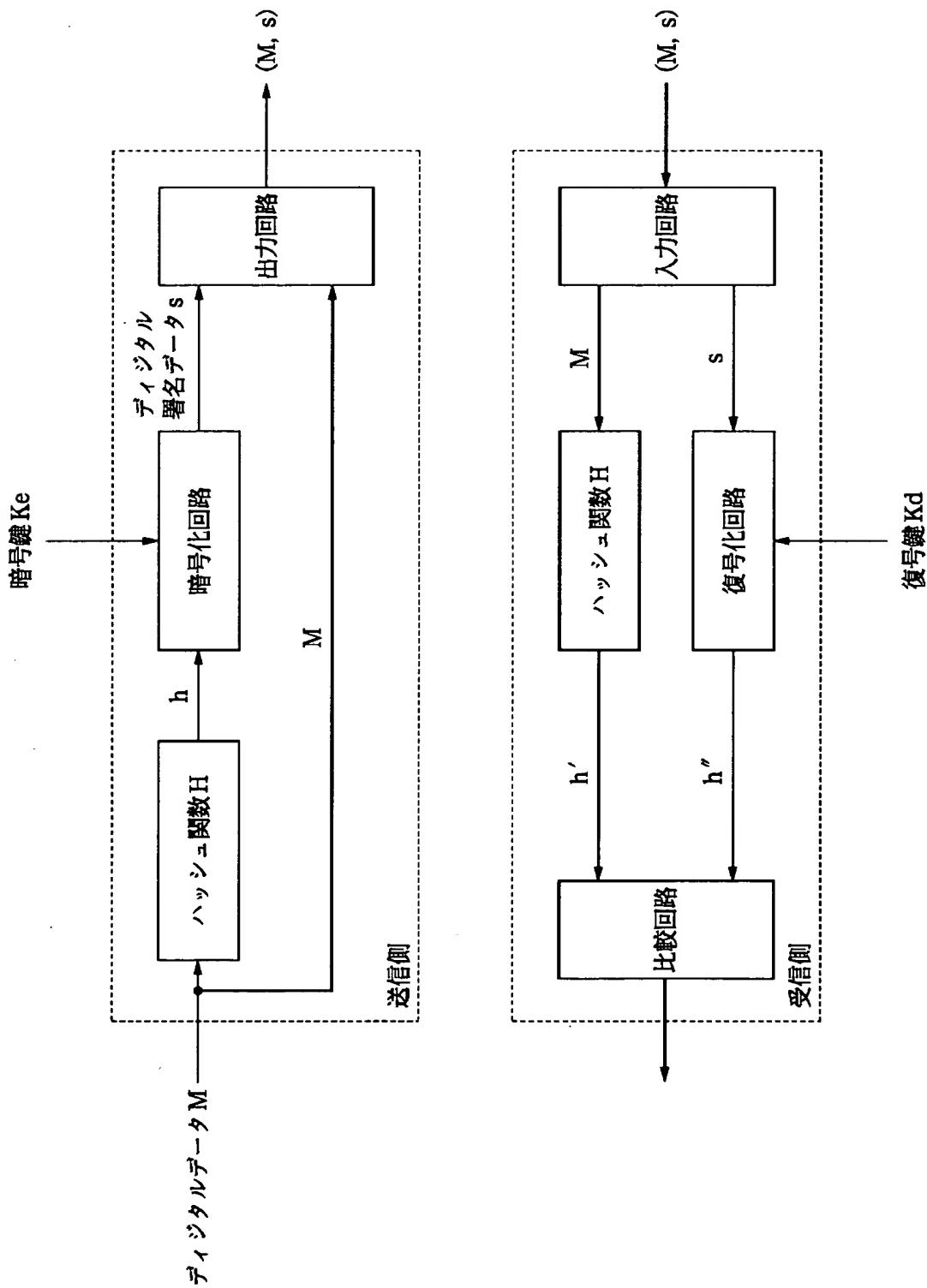
【図26】



【図27】



【図28】



【書類名】 要約書

【要約】

【課題】 ディジタルデータの正当性を検証することのできる技術を提供する。

【解決手段】 第1の画像処理装置10は、ディジタル画像11と秘密情報12とを用いて所定の演算を行い、その演算結果を用いて該ディジタル画像に対する不正な処理を検出するため署名データ13を生成する。第2の画像処理装置20は、そのディジタル画像11と秘密情報22とを用いて所定の演算を行い、その演算結果と上述の署名データ13とを比較してそのディジタル画像11に対する不正な処理の有無を検出する。

【選択図】 図1

認定・付加情報

特許出願の番号	特願2000-057077
受付番号	50000246613
書類名	特許願
担当官	第七担当上席 0096
作成日	平成12年 3月 7日

<認定情報・付加情報>

【特許出願人】

【識別番号】	000001007
【住所又は居所】	東京都大田区下丸子3丁目30番2号
【氏名又は名称】	キヤノン株式会社
【代理人】	申請人
【識別番号】	100090538
【住所又は居所】	東京都大田区下丸子3丁目30番2号 キヤノン 株式会社内
【氏名又は名称】	西山 恵三

【選任した代理人】

【識別番号】	100096965
【住所又は居所】	東京都大田区下丸子3丁目30番2号 キヤノン 株式会社内
【氏名又は名称】	内尾 裕一

【選任した代理人】

【識別番号】	100110009
【住所又は居所】	東京都大田区下丸子3丁目30番2号 キヤノン 株式会社内
【氏名又は名称】	青木 康

【選任した代理人】

【識別番号】	100069877
【住所又は居所】	東京都大田区下丸子3-30-2 キヤノン株式 会社内
【氏名又は名称】	丸島 儀一

次頁無

出願人履歴情報

識別番号 [000001007]

1. 変更年月日 1990年 8月30日

[変更理由] 新規登録

住 所 東京都大田区下丸子3丁目30番2号
氏 名 キヤノン株式会社